



U.S. Department of Interior  
Bureau of Land Management

## **Incident Response Plan 2.6**

Prepared by: Washington Office 840 – IT Security

Controlled Unclassified Information (CUI) For Official Use Only

## REVISION HISTORY

Ver	Date	Author	Description
1.0	09/04/2009	Don Nickel	Draft compiled/modified from multiple existing documents
1.1	04/29/2010	Don Nickel	Draft added 60 pages of tools SOP
1.2	05/09/2011	Kim Kelly	Update to Draft with process changes and document restructure for release to privacy and ITSM community, removal of the tool SOP sections added roles and responsibilities.
1.3	7/26/2011	Kim Kelly	Updates to tools list, finalize.
2.0	3/09/2012	Suzanne Wachter	Added Privacy Incident Response elements
2.1	6/29/2012	Suzanne Wachter	Additional revisions and additions to the Appendices
2.3	11/15/2013	Ashanti Murphy-Jones/ Chris Quamina	Review and Updates
2.4	3/11/2014	C. Garcia D. Levstik	Review & Updates
2.5	5/27/2014	C. Garcia D. Levstik	Review & Updates
2.6	6/23/2014	L. Eichenbaum	Submitted Final

# TABLE OF CONTENTS

1.0	Introduction.....	7
1.1	Purpose.....	7
1.2	Scope .....	8
1.3	OBJECTIVES .....	8
1.4	Maintenance.....	9
2.0	Organizing the IT Security Incident Response Capability .....	10
2.1	The Security Incident Response Team .....	10
2.2	The Privacy Incident Response Team .....	10
2.2.1	Overview.....	10
2.2.2	ITTF and BITTFs .....	11
2.3	BLM National Help Desk.....	11
2.4	The DOI Computer Incident Response Capability (DOI-CIRC) .....	11
2.5	Definition of an IT Security Incident .....	12
3.0	Handling an Incident.....	15
3.1	Phase 1: Detect the Incident.....	15
3.2	Phase 2: Analyze the Incident .....	15
3.2.1	OMB Incident Categories .....	16
3.2.2	US-CERT Incident Categories .....	17
3.3	Phase 3: Report the Incident .....	19
3.3.1	End User Incident Reporting .....	19
3.3.2	Notification to DOI-CIRC and US-CERT .....	19
3.3.3	Impact Notification .....	20
3.4	Phase 4: Contain the Incident.....	20
3.5	Phase 5: Eradicate the cause of the Incident.....	21
3.6	Phase 6: Recover from the Incident.....	22
3.7	Phase 7: Learn from the Incident.....	22
4.0	Privacy Information.....	24
4.1	OMB Memorandum M-07-16 .....	24
4.2	Privacy Loss Mitigation Strategy .....	24
4.2.1	Safeguarding PII.....	25
4.2.1.1	Physical Formats .....	25

4.2.1.2	Electronic Media .....	26
4.2.1.3	Training.....	26
4.2.1.4	Summary .....	26
4.3	Steps for Handling a Breach .....	27
4.3.1	Attempts to send PII .....	27
4.3.2	Incidents Involving Government Charge Cards .....	27
4.3.3	Incidents Involving PII sent via email .....	28
4.3.4	Incidents Involving Usernames and Passwords.....	28
4.3.5	Incidents Involving Sensitive BLM Data .....	29
4.3.6	Incidents Involving Lost or Stolen Equipment or Hardcopy Files.....	29
4.4	BITTF Requirements .....	29
4.5	Notification Considerations .....	32
4.6	External Breach Notification Policies .....	32
5.0	Handling Special types of incidents .....	34
5.1	Reporting Unsolicited email (aka SPAM .....	34
5.2	Government Furnished Equipment (GFE).....	34
5.3	Rootkit Incidents .....	35
5.4	Phishing, Social Engineering Attacks and Hoax Incidents .....	35
6.0	Roles and Responsibilities .....	36
6.1	BLM Computer Security Incident Response Team (BLM-CSIRT) .....	36
6.2	End User Responsibilities .....	36
6.3	Assistant Director, Information Resource Management (ADIR-IRM).....	37
6.4	The Bureau Chief Information Security Officer (BCISO) .....	37
6.5	Incident Response Manager .....	37
6.6	NOC DIRM Operational Security .....	38
6.7	Technical Support Subject Matter Experts .....	38
6.8	Physical Security/Facilities Management .....	39
6.9	IT Investigative/Forensics Expert .....	39
6.10	Evidence Custodian.....	39
6.11	Legal Liaison .....	40
6.12	Public Affairs/Media Relations .....	40
6.13	Human Resources .....	40
6.14	Privacy Office .....	40
6.15	System Owner .....	40

7.0	Regular Planning / Preparation.....	41
7.1	Define a baseline for all systems .....	41
7.2	Perform regular back-ups of data and software .....	41
7.3	Develop and document test procedures for each system.....	41
7.4	Incident Handling Tools .....	41
8.0	Incident Response Training, Testing and Exercises .....	43
8.1	Incident Response Training .....	43
8.2	Incident Response Testing and Exercises .....	43
8.3	Incident Handling Scenarios .....	43
8.4	Additional Incident Response Resources.....	43
9.0	Evidence Handling.....	45
9.1	Authorization .....	45
9.2	Emergencies .....	45
9.3	Gathering Evidence .....	45
9.4	Chain-of-Custody.....	45
9.5	Marking Evidence .....	45
9.6	Incident Records Retention and Destruction .....	45
9.7	Collecting Procedures.....	46
9.8	Evidence Gathering Materials .....	47
9.8.1	Law Enforcement .....	47
9.8.2	Reports and Information .....	47
10.0	External Contacts .....	48
10.1	Information Sharing with Outside Parties .....	48
10.2	Requests .....	49
11.0	Acronyms .....	50
	Appendix A: Quick reference on safeguarding pii, breach mitigation and incident management .....	51
	Appendix B: Incident Flow Charts .....	53
	Appendix C: Risk Assessment Model.....	63
	Appendix D: Standard Breach Reporting Template .....	65
	Appendix E: Sample Written Notification.....	68

Appendix F: Guidance: ESTABLISH Call Center - Privacy Act Breach .....	69
Appendix G: Sample After Action Report .....	73
Appendix H: PII Incident Response Quick Reference .....	74

## 1.0 INTRODUCTION

The Bureau of Land Management's (BLM) Information Technology (IT) systems and applications operate in a dynamic environment. This environment is subject to a variety of threats. Malicious code, viruses, Trojan horses, worms and attempts to gain unauthorized access are launched from anonymous locations around the world or from within BLM. Physical break-ins, denial-of-service attacks, and attempts to deface websites are also ever present threats. These threats present a need for a Bureau-wide IT security incident response plan.

The BLM is required by various federal and departmental regulations to ensure that all incidents involving BLM information are quickly and efficiently reported, investigated, and mitigated. In response to several high profile losses of personally identifiable information (PII), new federal and departmental mandates have been promulgated to ensure that incidents involving PII are properly managed in order to mitigate the loss of sensitive information.

This response plan was created in accordance with Office of Management and Budget (OMB) Memoranda on "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006,<sup>1</sup> "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16)," issued on May 22, 2007, the Department of the Interior (DOI) Privacy Loss Mitigation Strategy (PLMS), issued on May 22, 2007 and the requirements outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 3.

### 1.1 Purpose

This document describes the BLM process for responding to computer security incidents (to include incidents involving privacy information). The BLM Incident Response Plan establishes Bureau guidance and processes that form the IT security Incident Response capability. BLM National Interagency Fire Center (NIFC) employees follow the NIFC Incident Response Plan and report computer security issues or privacy violations Computer Security Incident Response Team (CSIRT).

Incident response comprises the full range of individual, managerial and technical activities required to deal with an IT security incident, including: notification, handling, recovery, analysis, and reporting. Incident response processes and standard operating procedures help to implement an ordered response to an often chaotic flood of events, facilitate cooperation and information exchange between parties affected by the incident and the BLM Computer Security Incident Response Team (CSIRT), and will support ongoing improvement to the security of BLM systems and applications. Incident Response may vary in approach depending on the situation, but will focus on the following objectives:

- Helping affected Bureau organizations recover quickly and efficiently from security incidents
- Minimizing impact due to loss, damage, or unauthorized alteration of information (regardless of classification) and/or disruption of critical computing services

---

<sup>1</sup> See [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

- Responding systematically, following proven procedures that will decrease the likelihood of reoccurrence
- Balancing operational and security requirements within realistic budgetary constraints
- Managing legal and media issues by the appropriate personnel

## 1.2 Scope

This document establishes processes and procedures for implementing a Bureau-wide IT security incident handling capability. It is based on The National Institute of Standards and Technology (NIST) SP 800-61 Rev 2, The Computer Security Incident Handling Guide and the IR and Privacy families of controls from NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Topics covered are roles and responsibilities necessary to implement incident management and incident handling and a review of seven phases of IT Security Incident Response: 1) Detect the Incident, 2) Analyze the Incident, 3) Report the Incident, 4) Contain the Incident, 5) Eradicate the Incident Cause, 6) Recover from the Incident, and 7) Learn from the Incident.

Large-scale incidents as described in Homeland Security Presidential Directive 5 (HSPD-5), the Homeland Security "National Incident Management System" (NIMS), and NIST SP 800-61 Rev 2 are escalated to and coordinated by the DOI Computer Incident Response Capability (DOI-CIRC) at the Departmental level.

Incidents involving the breach or potential breach of PII information are handled in accordance with Office of Management and Budget (OMB) Memoranda on "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16)," issued on May 22, 2007, and the Department of the Interior (DOI) Privacy Loss Mitigation Strategy (PLMS) Version 1, issued on May 22, 2007.

## 1.3 OBJECTIVES

The goals of the Incident Response Plan is to:

- Provide a 6AM to 6PM Mountain Time (Mon – Fri) support for security incidents within the BLM authorization boundary.
- Coordinate Bureau-wide responses to security incidents
- Facilitate communications to resolve computer security issues
- Establish and maintain a structured incident response and reporting process to address incidents
- Ensure that incidents are reported to DOICIRC in a timely manner
- Provide guidance, assistance, and feedback to NOC DIRM and DOI management in the form of "lessons learned" reports, trend analyses, alerts and advisories, and technical recommendations



#### **1.4 Maintenance**

The IT Security Program (WO-840 reviews the Incident Response Plan every two years or more frequently as triggered by the change/update process surrounding plan maintenance, a result from lessons learned or as deemed by management.

## 2.0 ORGANIZING THE IT SECURITY INCIDENT RESPONSE CAPABILITY

### 2.1 The Security Incident Response Team

The BLM Incident Response Team is subordinate to the DOI Computer Incident Response Capability (DOI-CIRC), which provides a coordinated, Departmental cross-Bureau approach to responding to computer security incidents.

The Incident Response Team is assembled on an incident-by-incident basis according to systems affected and skill sets necessary to resolve issues. The team is responsible for the hands-on tasks required to identify, contain, eradicate, recover, and follow-up on an IT security incident. This team handles IT security incidents from start to finish, unless escalated. The team is comprised of the BLM CSIRT members and any technical or ad hoc Subject Matter Experts and NOC DIRM Operational Security as needed. The BLM CSIRT attends to organizing and coordinating the response.

For all Incidents (to include possible PII or Privacy Incidents); for all Contingency Events; or for an immediate need to contact BLM IT Security, use any of these means:

**Phone number:** Contact BLM IT Security by phone at: 303-236-0611 (this number rings on all of the desks) or,

**E-mail:** Email IT Security at:  
BLM\_INCIDENTS\_IT\_SECURITY@blm.gov (send encrypted if reporting any sensitive or PII information)

BLM CSIRT members from WO-840 will create a DOICIRC ticket

**After-hours:** BLM CSIRT Manager (WO-840) cell phone: (303) 828-8646.

### 2.2 The Privacy Incident Response Team

#### 2.2.1 Overview

The Office of Management and Budget (OMB) Memoranda on “Recommendations for Identity Theft Related Data Breach Notification,” issued on September 20, 2006,<sup>2</sup> and “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16),” issued on May 22, 2007<sup>3</sup> required Bureaus to provide guidelines and guidance regarding the safeguarding of PII, how to handle a breach of PII, and what employees can do to ensure PII is protected.

---

<sup>2</sup> See [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

<sup>3</sup> See <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf> (Hereinafter OMB M-07-16).

### 2.2.2 ITTF and BITTFs

The DOI Identity Theft Task Force (ITTF) is the departmental task force responsible for providing planning, policy, breach incident coordination and guidance regarding the actual and potential breaches of PII within the custody of the Department. The ITTF will also meet on an ad hoc basis to address incidents of breach and to update the DOI's Privacy Loss Mitigation Strategy (PLMS). In the event of a breach involving multiple Bureaus, the ITTF serves as liaison and decision making body between the functional area(s) affected and other organizations and Bureau Identity Theft Task Force (BITTF). If a significant loss occurs, the DOI ITTF will become involved upon notification by reporting official(s). At a minimum, the DOI CIO and Privacy Officer will determine whether the DOI ITTF should assume control of handling the incident. The membership of the DOI ITTF includes: Senior Agency Official for Privacy (SAOP), Departmental Privacy Officer, Chief Information Officer (CIO), Chief Financial Officer (CFO), Solicitor, Inspector General (IG), Chief Information Security Officer (CISO), and the Legislative Affairs Officer.

The BITTFs are the Bureau-level equivalent of the ITTF. The BITTFs are expected to be the first responders to incidents that take place within the Bureau. The State/Center Privacy Officer where the incident occurs must schedule a BITTF within 3 business days of the incident. Information regarding an incident must be immediately forwarded to the Bureau Privacy Act Officer. The membership of the BITTFs will be determined by the Bureau Chief Information Security Officer (BCISO), but must include the BCISO or designated representative, Bureau/Office Privacy Officers, NOC DIRM Operational Security Zone Managers.

### 2.3 BLM National Help Desk

The BLM National Help Desk (NHD) is responsible for creating Remedy Help Desk tickets and assigning the Remedy tickets to the BLM CSIRT, processing requests that come directly from users across the Bureau. Confirmed or suspected loss of PII or privacy incidents should be sent directly to the BLM CSIRT via encrypted email to [BLM\\_Incidents\\_IT\\_Security@blm.gov](mailto:BLM_Incidents_IT_Security@blm.gov). BLM National Helpdesk should NOT enter loss of PII tickets into the Remedy system. National Help Desk contact information:

**Phone number:** 800-BLM-HELP (800-256-4357)

**E-mail:** [1800blmhelp@blm.gov](mailto:1800blmhelp@blm.gov)

**Web:** <http://1800blmhelp.blm.gov>

### 2.4 The DOI Computer Incident Response Capability (DOI-CIRC)

DOI-CIRC is a Departmental incident response capability that provides departmental-level support for incident handling. The DOI-CIRC serves as a central clearinghouse for Interior incident information and is a source of assistance for the coordination of incidents. The DOI-CIRC reports incidents to US-CERT and/or Office of the Inspector General and/or law enforcement, and provides services such as threat analysis and virus alerts to the Bureaus.

Users need to contact DOI-CIRC only in the event that they could not reach the BLM CSIRT Manager after hours.

**DOI-CIRC Analyst:** 703-648-5655

**Email:** doircirc@ios.doi.gov

**Web Page:** <https://ensupport.doi.gov> (End users would never use this; it is only accessible to certain members of the BLM CSIRT.)

## 2.5 Definition of an IT Security Incident

The Department of the Interior (DOI) defines a computer security incident as “the act of violating the explicit or implied security policy of a computer system.” Incidents may compromise the availability, integrity, and/or confidentiality of Bureau IT and telecommunications resources. A reportable incident is defined by BLM to include, but is not limited to:

- The loss or suspected loss of any Personally Identifiable Information (PII) as defined in OMB 07-16 and OMB 06-19: “Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.” (Note: this loss may occur as a result of a ‘physical loss’ such as losing a laptop or physical media or a ‘logical loss’ where data was transferred electronically in the clear where the potential exists to be viewed by unauthorized parties.)
- Attempts (failed or successful) to gain unauthorized access to a system or its data
- Successful introduction of a virus/worm into a network
- Detection and elimination of malicious code before infestation (Isolated incident)
- Presence of, exchanging or viewing pornographic material on or with a government computer or resource
- Possession, viewing, transmission or downloading child pornography
- Defaced web sites
- Unexplained computer system crashes (unless proven to not be security-related)
- Disruption or denial-of-service (no matter how successful or unsuccessful)
- Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service
- A person gaining logical or physical access without permission to a federal agency network, system, application, data, or other technical resource

- A person violating acceptable use of any network or computer use policies
- Unauthorized use of IT services or telecommunications resources
- Unauthorized changes to system hardware, firmware, or software
- Unauthorized changes to system or application configuration
- Using someone else's user ID and password
- User Account Compromise
- Changing or copying data without authorization
- Damaging or unauthorized destruction of hardware or software
- Deliberately slowing the processes of the computer system
- Violating copyright laws
- Deliberately erasing data that should not be deleted
- Any loss of Government Furnished Equipment (GFE) containing BLM information electronically stored, such as Smartcards, laptops, Blackberries, flash/thumb drives, removable hard drives, Personal Digital Assistants, cell phones, or any other portable electronic devices
- Loss or compromise of sensitive information
- Communicating a threat to life or limb via e-mail
- Compromised DNS server
- Bypassing firewall access control lists (success or failure)
- Compromised root or system administrator accounts
- Non-authorized scanning or intrusion of government information system
- Unauthorized network port scans
- Anything out of the ordinary that involves a government computer system
- Using unauthorized peer-to-peer (P2P) file sharing software such as LimeWire
- Operating a business on government computer systems
- Day trading (stocks)

- Social Engineering (i.e. phone calls or emails asking for user names and passwords)
- An unauthorized administrative account
- Gaps in system logs
- Spam, fraudulent or threatening email
- *Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review that may be indications or precursors to an incident. An indication is a sign that an incident may have occurred or may be occurring now. A precursor is a sign that an incident may occur in the future. For example:
  - A network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server
  - Antivirus software alerts when it detects that a host is infected with a worm
  - Web server crashes
  - Users complainants of slow access to hosts on the Internet
  - A system administrator sees a filename with unusual characters
  - A host records an auditing configuration change in its log
  - An application logs multiple failed login attempts from an unfamiliar remote system
  - A large number of bounced e-mails with suspicious content
  - A network administrator notices an unusual deviation from typical network traffic flows

## **3.0 HANDLING AN INCIDENT**

The BLM CSIRT will follow a seven-step process to provide incident handling services. The steps or phases are as follows:

### **3.1 Phase 1: Detect the Incident.**

The first phase of the incident response process, detect the incident, involves receiving warning of a possible IT security incidents which may come from several sources, including:

- Reports from Bureau or Department IT systems and network administrators
- Alerts by intrusion detection systems (IDS) or other network monitoring appliances or tools
- Notification from the DOI-CIRC, US-CERT or other trusted sources of a potential high risk vulnerability
- Reports by end users and/or NOC DIRM Operational Security Team During normal system operations any system or information anomalies discovered need to be evaluated to determine if it meets the criteria of a security incident. See Section 2.5 for the definition of an IT Security Incident.

Upon discovery of anything defined as a “reportable event” and considered a potential or confirmed security incident, the National Help Desk assigns the ticket to the BLM CSIRT, initiating the incident response process. The BLM IT Incident Response Manager may designate an Incident Response Team or an Incident Handling Group, if necessary. The Incident Response Team may include NOC DIRM Operational Security Team, and if necessary, other Subject Matter Expert’s (SME) for that particular incident. The Technical Lead then notifies the Incident Response Team members and keeps an incident log with any technical updates.

### **3.2 Phase 2: Analyze the Incident**

The WO-840 Staff gathers facts about the incident, analyzes the information, identifies entities affected by the incident, assesses the severity and extent of damage, and assigns an incident threat level. Throughout the process, information is captured and the incident response documentation is carefully maintained.

Facts about the incident are collected from a variety of sources. End users, help desk personnel, systems and network administrators, etc. provide the information needed to understand the incident and develop a successful response. The collected information is analyzed to understand the nature of the incident, assess the severity, current impact, and potential impact. The group analyzes the information to identify entities impacted, directly and indirectly, by the incident.

Finally, the group will work together to assess the incident, determine the incident threat level and decide on a preliminary course of action based upon the incident severity. For low severity incidents, the response can be resolved within the respective zones. For medium, high and critical severity incidents, the response should be coordinated with BLM CSIRT.

Timely reporting of incidents is essential. The BLM CSIRT formally reports to other entities based on the category, severity and frequency of an incident. BLM CSIRT follows the Office of Management and Budget (OMB) and U.S. CERT categories which are detailed below.

### 3.2.1 OMB Incident Categories

Severity	Severity Definition	Examples of Incidents	BLM National Help Desk Reports To	Timeframe Not to Exceed
OMB Critical	Loss of Personally Identifiable Information (PII) / Privacy Act (PA)	Leak or loss of any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.	BLM-CSIRT	15 minutes
Critical	The threat poses significant risk to BLM resources or other outside computer systems and requires immediate action.	E-mail containing a threat to life or limb	BLM-CSIRT	One hour
		Denial of Service/Distributed Denial of Service Attacks.(no matter how successful or unsuccessful)	BLM-CSIRT	One hour
		Compromised DNS server	BLM-CSIRT	One hour
		Web site defacement	BLM-CSIRT	One hour
		Bypassing firewall access control lists	BLM-CSIRT	One hour
		Possession, viewing, transmission or downloading child pornography	BLM-Law Enforcement	One hour
		Root or system administrator account compromised	BLM-CSIRT	One hour
		Successful introduction of a virus/worm into a network – widespread, not an isolated incident.	BLM-CSIRT	One hour
High	The threat significantly impacts BLM computer resources and requires immediate action.	Unauthorized scanning or intrusion of critical system	BLM-CSIRT	One hour
		Involves a computer system that is classified as trust, national critical information infrastructure, financial or mission critical. Impacts devices accessible from the Internet	BLM-CSIRT	One hour
		Detection and elimination of malicious code before infestation. (Isolated incident)	NOC DIRM Ops Security	One hour
Medium	The threat impacts BLM computer resources and	Unauthorized scanning or intrusion into non-critical system	BLM-CSIRT	One hour



Severity	Severity Definition	Examples of Incidents	BLM National Help Desk Reports To	Timeframe Not to Exceed
	requires attention as soon as possible. For example, a Medium threat level response would not require action after normal business hours, but is important enough that responding should be made a priority in the normal course of operations.	Successful network attacks that result in Denial of Service (DOS)	BLM-CSIRT	One hour
		Using unauthorized peer-to-peer file sharing software such as napster	BLM-CSIRT	One hour
		Operating a business on government computer systems	BLM-CSIRT HR	One day
		Day trading (stocks)	BLM-CSIRT HR	One day
		Exchanging or viewing pornography	BLM-CSIRT HR	One day
		User Account Compromise	NOC DIRM Ops Security	One day
Low	Does not immediately impact BLM computer resources but warrants some research and possible action.	Unauthorized network port scans	BLM-CSIRT	One day
		Social Engineering: Phone calls or emails asking for user names and passwords	NOC DIRM Ops Security	One day
		An unauthorized admin account	NOC DIRM Ops Security	One day
		Presence of cracking tools	BLM-CSIRT	One day
		Gaps in system logs	BLM-CSIRT	One day
		Spam or fraudulent email	NOC DIRM Ops Security	One day

### 3.2.2 US-CERT Incident Categories

In support of the Federal Information Security Management Act (FISMA), Federal agencies are required to report all computer security incidents to US-CERT based on the incident categories and reporting timeframes detailed in the US-CERT Federal Concept of Operations (CONOPS). These incident categories and descriptions were developed and agreed upon by an interagency body during the development of the US-CERT Federal CONOPS. The Office of Management and Budget (OMB) released a memorandum in May 2007 directing all Federal agencies to adhere to the incident categories and their specified timeframes when reporting incidents to US-CERT. The table below reiterates the US-CERT incident categories and reporting timeframes as of January 2008.

For Reporting purposes, the most stringent reporting requirement is the requirement that should be used.

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	A person gains logical or physical access without permission to a federal agency network, system, application, data, or other technical resource.	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Inappropriate Usage	A person violates acceptable use of any network or computer use policies.	Weekly
CAT 5	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Note: Pornography and Child Pornography are treated as distinct and separate categories.

### **3.3 Phase 3: Report the Incident**

End user reporting of an incident should occur immediately upon discovery to the National Help Desk, BLM IT Security (WO-840) or immediate supervisor. It is a key factor in the process. Once notified that an incident occurred, the BLM CSIRT performs formal notification within certain timeframes to DOI-CIRC and US-CERT based on the severity of the incident and its potential impact. They also perform potential impact notification to other offices that may be affected by an incident currently happening.

Secure reporting mechanisms (e.g., secure phone, secure fax, encrypted e-mail) are to be used whenever sensitive information is being disseminated.

#### **3.3.1 End User Incident Reporting**

End users of BLM systems, whether federal employees or government contractors, are required to immediately report potential, suspected or confirmed reportable security incidents (defined in section 2.5) and any system anomalies. They are also expected to give their full cooperation to the Incident Response Team during an IT security incident. All users of Federal IT resources are accountable for all activity performed under their unique user ID. Report incidents to National Help Desk or directly to [BLM\\_INCIDENTS\\_IT\\_SECURITY@blm.gov](mailto:BLM_INCIDENTS_IT_SECURITY@blm.gov) as described in sections 2.1 and 2.3. For questions or further local guidance on incident reporting, contact the NOC DIRM Ops Security.

Follow the instructions provided by the NOC DIRM Ops Security for the reported incident. If the NOC DIRM Ops Security, National Help Desk, or BLM IT Security (WO-840) is not immediately available, use the following general guidance until security personnel are contacted:

- If a user believes their system has been infected with malicious code (virus/worm/Trojan) and is connected to a LAN, disconnect the network cable from the back of the computer until specific instructions are received by authorized personnel.
- Potential emergency situations are considered critical and should be reported immediately to BLM CSIRT or if discovered after hours to the BLM CSIRT Manager as defined in section 2.1. Emergency situations include: immediate threat to life or property; violation of any law (such as child pornography); disclosure of or unauthorized access to sensitive information; involvement of a computer system or stored information categorized as trust, national critical information infrastructure or financial; widespread effect within BLM or involvement of multiple bureaus; or, impact on devices accessible from the Internet.

#### **3.3.2 Notification to DOI-CIRC and US-CERT**

BLM CSIRT team members will perform the notification to DOI-CIRC and US-CERT based on the category, severity and frequency of an incident. They follow both OMB and US-CERT categories described in Phase 2 above and will escalate to US-CERT using the procedures below:

US-CERT standard business hours are 7AM – 7PM Eastern Standard Time (EST) Monday – Friday.

If it is determined that the incident should be escalated to US-CERT, call DOI-CIRC at 703-648-5655, and provide the ESP/DOI-CIRC ticket number to the DOI-CIRC analyst. The DOI-CIRC analyst is responsible for creating the corresponding US-CERT ticket and populating the original ESP/DOI-CIRC ticket with the newly created US-CERT ticket number once available.

US-CERT escalation after hours – After hours are considered after 7PM and before 7AM Monday – Thursday Eastern Standard Time (EST) as well as 7PM Friday thru 7AM Monday and all Government holidays.

If it is determined that the incident should be escalated to US-CERT after hours, call the Verizon GNOSC at 1-866-376-6672, and provide the ESP/DOI-CIRC ticket number to the GNOSC analyst. The GNOSC analyst is responsible for creating the corresponding US-CERT ticket and populating the original ESP/DOI-CIRC ticket with the newly created US-CERT ticket number once available.

The current standard for reporting compromise of PII or other widely impacting incidents to US-CERT is 1 hour after they are discovered. With this in mind, contact the DOI-CIRC or GNOSC as soon as the Remedy/DOI-CIRC ticket is created.

### **3.3.3 Impact Notification**

Impact notification is the process of warning other IT personnel at BLM offices or organizations that they could potentially be affected by an IT security incident currently taking place or which has already occurred at a BLM site. The goal is to enable IT security personnel within other potentially affected organizations to minimize or pre-empt further losses of confidentiality, integrity, or availability of systems or data. In this way negative publicity, loss of reputation, legal liability, and/or national epidemics might be prevented or mitigated.

Due to the high-speed proliferation of malicious intrusions, impact notification is not to be delayed. Impact notification is to be overseen by the Incident Manager but may be delegated to anyone with access to a telephone, e-mail, or fax. The person performing the impact notification will need to be equipped with a contact list and a description of what is currently known about the incident to relay to those who may be impacted. This process can be greatly expedited by maintaining a current contact list of IT personnel at sites that are connected to the network.

For reporting bomb threats and other serious emergency procedures, follow local Emergency Plan Procedures. Report physical incidents to Federal Protective Service (FPS) or the law enforcement entity responsible for the facility.

## **3.4 Phase 4: Contain the Incident**

The purpose of containment is to limit the scope and magnitude of an IT incident. Containment usually consists of short-term, tactical actions intended to remove access to compromised systems, limit the extent of current damage, and prevent additional damage from occurring.

Each incident presents a different situation and will need to be handled accordingly. This section provides general guidelines. All steps taken must be fully documented. End users should contact the National Help Desk first.

**NOTE: For incidents involving criminal activity—DO NOT issue any commands on the affected system until authorized to do so by the BLM CSIRT or by law enforcement!** Some commands could inadvertently destroy critical evidence in system log files. In order to ensure the integrity and accuracy of evidence, the state of the system must remain unchanged until carefully planned and executed steps can be taken by someone knowledgeable on preserving computer system evidence intact.

- Collect information - As appropriate, prior to disconnecting the system from the network, obtain a system generated list of open network connections and running processes. For example, running netstat on Windows systems will provide a list of all open inbound and outbound connection sources, and their ports. This evidence can be extremely useful for forensic analysis.
- Isolate the system(s) affected – Disconnect network connections to affected system(s) or unplug the network cable to prevent further remote access. While isolating the affected system(s) is the quickest and most effective way of containing an incident, it can have significant impact on the Bureau's business operations.
- Change firewall filtering rules, access control lists, etc. as necessary - firewall rules may need to be changed to prevent access to the system.
- Disable accounts – to address medium or low level threats, accounts can be disabled to prevent further unauthorized access.
- Disable services – turn off services such as telnet, ftp, etc.

In extreme cases, it may be advisable to shut down the computer system. However, it is preferable to isolate the computer from the network to allow a computer security specialist to preserve evidence.

If a virus is suspected, immediately isolate the infected machines from the local area network by unplugging the network cable from the back of the infected computers. Gather all electronic media that may have been used in the infected computers.

**NOTE: In the event that a BLM computer security incident is suspected of being the result of criminal activity, great care must be taken to preserve the trail of evidence.** Preservation of evidence must occur before proceeding otherwise vital data needed for an investigation will be lost, overwritten, or otherwise destroyed. The BLM Security Staff (WO-840) should contact BLM OIG for support in this instance.

### 3.5 Phase 5: Eradicate the cause of the Incident

Following containment, the incident's cause must be eradicated from the affected system(s). Eradication involves removing any of the incident's artifacts. This task can be complicated, when multiple threats, platforms, and operating systems are involved.

If the cause of the incident is some type of malicious software, such as a virus or worm, eradication requires removing the code from all affected systems and media, using an updated version of anti-virus software and undoing any unauthorized changes to system settings and configurations.

**NOTE:** Without well-defined and carefully documented baseline system configurations and comprehensive file integrity data, it is next to impossible to eradicate malicious code and its unauthorized changes to the affected system(s) with any degree of confidence.

The importance of cleaning and/or reformatting all infected media cannot be overstated. It is important to carefully observe and/or review the virus cleanup logs to determine if additional measures are needed. Frequently, systems are re-infected due to lack of diligence in checking all media and files.

Additionally, if a previous backup of the system is to be used to restore newly infected files, be sure that it is also free of malicious software (i.e., a “trusted backup”) and its effects. It may be necessary to return to the original distribution media and re-customize the system. After eradication, a new backup of the system must be made.

Eradication is not complete until the vulnerability originally exploited is addressed.

Vulnerabilities must be isolated and, if possible, removed to prevent or discourage recurrence. If the exploited vulnerability cannot be removed, it must be mitigated through the use of additional controls and/or monitoring to protect the system from future exploitations of that vulnerability.

Unless there is an immediate threat to the security of data, great care is to be taken to collect all necessary information about the compromised system(s) and the cause of the incident, as they will likely be lost when eradicating the incident.

Once the incident has been eradicated, the response team moves to Phase Six: Recovery.

### **3.6 Phase 6: Recover from the Incident**

Recovery from an incident involves returning systems to normal operation and will vary based on the incident particulars. Systems that have been taken down or otherwise compromised require WO-840 IT Security (BCISO) approval before being returned into production.

Before beginning recovery, ensure that the hard drives of the compromised system(s) are copied before repairs are made. This will allow the environment to be frozen for future research or as possible evidence.

Recovering normal operations may involve repairing system and application software by undoing unauthorized changes, restoration from backup media, or rebuilding from original media. Recovery may be as simple as reconnecting a system taken off-line during the containment phase or as complicated as rebuilding from original media multiple systems supporting a web application

Repairs such as patch installations and password changes are performed to secure the system and avoid recurrence. If the system cannot be repaired, a clean restore or rebuild must be performed and the system patched to prevent further incidents. After repair, rebuild, or restore is complete, the systems are then tested to ensure that all appropriate repairs have been completed and the system is operating correctly. System tests must ensure that the factors leading to the incident have been eliminated.

After the integrity of restored data and files are verified, reconnect the system(s) to the network.

Upon completion of the Recovery Phase, the response team moves to Phase Seven: Lessons Learned from the Incident.

### **3.7 Phase 7: Learn from the Incident**

After an incident has been resolved, a post-incident analysis, also known as a “Lessons Learned” or an “After-Action” report is conducted as soon as feasible, so that lessons learned can be adopted and procedures updated, as needed (see Appendix G). The analysis is to consist of a review of all responses compiled during the incident to ascertain how such an event might be

prevented or minimized in the future. A damage analysis of all IT incidents is to be initiated immediately after assessment, containment and recovery actions are complete.

The following kinds of incident information are to be examined during the analysis:

- How did the incident start?
- Which vulnerabilities were exploited?
- What information/system was compromised?
- How was access gained?
- How did the incident present itself?
- How was the incident resolved?
- Are existing controls adequate, or do they require modification?
- Do vulnerabilities still need to be closed?
- What documents and/or procedures need to be updated?
- Did the communications and reporting channels function adequately?
- Are existing IR procedures adequate, or do they require modification?
- What should be done better next time?

A follow-up analysis may result in the need for:

- Alerts or warnings to be issued about how to reduce vulnerabilities that were exploited during the incident.
- Updating the Incident Response Standard Operating Procedures.

The results of the analysis may also be used to:

- Ascertain the impact to BLM resulting from the handling and resolving of the incident. Although this may be difficult to quantify, some measure of its performance and beneficial effect may be useful in determining the future scope and direction of the Incident Response Team.
- Develop ideas for improvement such as modifying system security and configuration guidelines, improving user security awareness, modifying IT security policies and procedures, or modifying security incident response procedures.
- Identify specific training needs for improving incident response capabilities.

The Incident Manager initiates the process of estimating the overall economic impact of the incident to the office/mission area and to BLM in cooperation with the System Owner/Business Manager. This estimate is to quantify the impact in terms of loss of system(s) availability, loss of response capability to customers, cost of equipment/software to repair, and hours of personnel associated with the repair or restoration of the system(s). The damage assessment report is reviewed and agreed to by the System Owner/Business Manager prior to inclusion in the IT Incident Report.

## **4.0 PRIVACY INFORMATION**

### **4.1 OMB Memorandum M-07-16**

OMB Memorandum M-07-16 reiterates the existing security requirements, including: assigning impact levels to all information and information systems, implementing minimum security requirements, certifying and accrediting all information systems, and training employees on their privacy and security roles and responsibilities. This section summarizes the requirements set forth in M-06-16 and M-07-16. These requirements include:

- Reviewing current holdings of all PII and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete; and reducing them to the minimum necessary for the proper performance of a documented agency function;
- Developing and making public a schedule by which system and record owners will periodically update the review of their holdings;
- Reducing the use of Social Security Numbers (SSNs) in agency systems and programs and identifying instances in which collection or use of the SSNs is superfluous;
- Publishing a routine use for appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach;
- Using only NIST certified cryptographic modules encrypt all data on all mobile computers and devices that carry sensitive data;
- Allowing remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Using a “time-out” function for remote access and mobile devices requiring user re-authentication after no more than thirty minutes of computer inactivity;
- Logging all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days of its use, or is still required;
- Ensuring all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities; and
- Informing employees of Agency’s low tech safety measures they can use to ensure protection of PII.

### **4.2 Privacy Loss Mitigation Strategy**

The section outlines procedures to be taken to prevent a breach of PII and in response to a breach of PII. It follows the PLMS published by the Department of Interior.



### 4.2.1 Safeguarding PII

Personally Identifiable Information (PII) and Privacy Act (PA) information are jointly referred to as “Privacy Information” for the purpose this guidance. Privacy Information includes such information such as: home addresses, home telephone numbers, personal cell phone numbers, logins and associated passwords, government and personal banking information (i.e. credit card numbers, account numbers, etc.), Social Security Numbers (SSN) (even if only the last four digits are displayed), etc. The following guidance applies to Privacy Information in all formats, including (but not limited to) paper, electronic, video, and audio. It also applies to employees own personal Privacy Information as well as the Privacy Information of others. All BLM employees have an affirmative duty to protect Privacy Information. Failure to properly protect Privacy Information may result in administrative actions (from computer login being disabled to suspension). The following procedures apply to all Privacy Information.

#### 4.2.1.1 Physical Formats

All files/folders containing documents with Privacy Information must be secured in locked cabinets or locked rooms when not in use. Each cabinet storing Privacy Information must have a warning label affixed to the front of the cabinet/door. (See BLM Form S-137, “Warning – Access To These Records Is Limited To Authorized Personnel.”)

Examples of records that need to be protected include:

- Supervisors’ records pertaining to employees, time and attendance records
- Employee Performance Appraisal Plans (EPAPs)
- Emergency contact cards/home phone lists
- Credit card statements
- Hard copy travel authorizations must be safeguarded

All file folders which contain documents with Privacy Information should have a “Notice of Restricted Access” either stapled on the cover or placed inside the file. This form may be reproduced locally.

Employees who work with Privacy Information must take precautions to avoid exposing protected information to others who do not have a “need to know.” All Privacy Information must be secure when the responsible employee is away from his/her work area (e.g., lunch, break, meeting, etc.).

Employee forms which contain any Privacy Information must be distributed in a sealed Special Attention Mail envelope (i.e. blue envelope). Examples of such forms are SF-50, Notification of Personnel Action; DI-3100 EPAP; SF-2823, Designation of Beneficiary, credit cards statements, etc.

#### **4.2.1.2 Electronic Media**

All agency data stored on portable media (external hard drives, thumb/flash drives) must be encrypted. All laptops must have National Institute of Standards and Technology (NIST) certified encryption. Contact IT Security personnel for encryption requirements and assistance.

All electronic transmissions (i.e. emails), including the body of the email and any attachments, sent from a Government computer to outside of the DOI network are viewed in clear text by DOI IT security staff. Those e-mails containing Privacy Information, such as logins and/or passwords, SSNs, credit card information, etc. will be flagged by DOI and reported to WO-840 personnel and the BLM Privacy Officer as a PII Breach. These types of breaches may result in the affected employee's BLM computer login being disabled or other adverse administrative actions being taken.

Privacy Information may only be sent outside the network via email when encrypted or in a password protected document (provided the password is sent separately). This includes business and personal logins and/or passwords sent to an employee's own personal private email. Contact the NOC DIRM Ops Security for assistance.

W-2s and other personal documents (such as Leave and Earning Statements and credit card statements) that contain personal Privacy Information about a user and their own family may not be sent outside the network via email.

#### **4.2.1.3 Training**

Each State, District and Field office should ensure that their employees are properly trained in the handling of PII data. Information about the Privacy Act should be regularly refreshed by employees during their annual privacy training module in the FISSA training, as well as other Bureau training and awareness programs.

#### **4.2.1.4 Summary**

The following steps must be taken to safeguard PII.

- Physically secure or lock up an area, document or equipment that contains PII.
- When working with documents containing PII (travel documents, leave information, personal performance ratings, etc.), ensure they are in folders and/or have a cover sheet with proper notification (see the Privacy Act Warning Notice at [http://www.mydoi.doi.net/ocio/imd/ocio\\_privacy\\_guidelines.html](http://www.mydoi.doi.net/ocio/imd/ocio_privacy_guidelines.html).)
- Do not leave laptops, or any other electronic devices that might contain PII unattended.
- Do not take documents with PII out of the Federal office environment unless they are secured and labeled in accordance with Federal requirements.
- Ensure the Federal records are always in government possession; do not email the records to a personal email address to work on at home (this takes the control of the documents out of agency hands). Federal records should NEVER leave the control and ownership of the agency!

### **4.3 Steps for Handling a Breach**

Different types of potential breaches of privacy information require different steps to be taken in response. These steps are based on the nature of the information breached and whether the information left BLM/DOI networks. In situations where the information has left DOI networks (i.e. an actual breach has occurred) US-CERT must be notified within one (1) hour of discovering the breach. The entry of the information regarding the breach into the DOI-CIRC system satisfies this notification requirement.

Unique situations not listed below should be handled in accordance with the procedures listed for the most comparable situation. If it is suspected that the information was compromised or was attempted to be compromised with the intent to commit a crime or in furtherance of suspected criminal activity, contact law enforcement immediately. Contacting law enforcement does not negate or satisfy the requirement to notify US-CERT within one hour of discovering an incident.

#### **4.3.1 Attempts to send PII**

All emails being sent using the BLM/DOI networks are scanned by the Symantec Messaging Gateway (SMG). If the email is suspected of containing PII, the email will be stopped and the individual sending the email will receive an email notice that the email was not delivered because it may contain PII. If the email does not contain PII or other sensitive BLM data, the individual can enter a helpdesk ticket to have the email released for delivery.

If the email does contain PII or other sensitive BLM data, an incident report will be entered into Remedy by the WO-840 group. Instances of personal PII will not be reported. The Privacy Officer for the State or Center owning the network used to send the email has the obligation to ensure the individual sending email is reminded of the prohibition against sending PII via email unencrypted or password protected. A copy of this policy or of IM 2012-0504 can also be provided as a reminder. The email should be deleted off the system. And, if appropriate, the individual can be required to re-take FISSA+ training. If the individual is required to re-take the FISSA+ training and does not accomplish that training within three (3) business days, then the individual's network access should be restricted.

After these actions are taken, the incident should be closed in the Remedy system.

#### **4.3.2 Incidents Involving Government Charge Cards**

This section assumes that the information left secure BLM/DOI networks without being stopped. If the information was stopped by Symantec Messaging Gateway, take the actions listed in section 4.3.1 above. Incidents involving government charge cards will be entered into DOI CIRC (usually by the WO-840 group). The State or Center Privacy Officer responsible for the network used to send the government charge card numbers has the primary responsibility for handling these incidents; however, they should work closely with individual responsible for the government charge card program for their state.

Any individual whose Government Charge Card number was sent should be notified of the potential compromise. All copies of the email should be deleted from all email folders (inbox, deleted emails and any other folders to which the email may have been saved). Whoever manages the government charge card program for the location where the incident occurred should be notified as well as the credit card company. A determination will need to be made by the concerned parties as to whether the affected cards should be cancelled.

The Privacy Officer for the State or Center owning the network used to send the email is responsible for ensuring the individual sending email is reminded of the prohibition against sending PII or sensitive BLM data via email unencrypted or password protected. The individual can be required to re-take FISSA+ training, if appropriate. If the FISSA+ training is not accomplished within three (3) business days, then the individual's network access should be restricted. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate. Once all necessary action has been completed inform the WO-840 group so they can close the incident in DOI-CIRC.

#### **4.3.3 Incidents Involving PII sent via email**

Incidents involving actual compromise of PII sent via email will be entered into DOI CIRC by WO-840 personnel. If possible, all copies of the email and any attachments are deleted, as appropriate from the inbox, deleted email folder, computer, servers, etc. A BITTF may need to be convened (see Section 4.4). If a determination is made by the BITTF that notification is warranted, notify the individual(s) whose PII has been compromised using one of the approved methods. The forms of notification must be done in accordance with the DOI PLMS and OMB M-07-16. Telephonic notification may be used when there are a small number of affected individuals and the situation dictates urgency. First-Class Mail notification is the most widely accepted. Notifications should be mailed separately from other information and marked "Important Notification." Email notification may be used if individuals have consented to the use of email as a primary means of communication with agency and no mailing address is known. If unique circumstances exist requiring exceptions be made to the above directions or alternative methods of notification need to be used contact the Bureau Privacy Act Officer for approval.

The Privacy Officer for the State or Center owning the network used to send the email is responsible for ensuring the individual sending email is reminded of the prohibition against sending PII or sensitive BLM data via email unencrypted or password protected. The individual can be required to re-take FISSA+ training, if appropriate. If the FISSA+ training is not accomplished within three (3) business days, then the individual's network access should be restricted. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate. Once all necessary action has been completed inform the WO-840 group who will close the incident in DOI-CIRC.

#### **4.3.4 Incidents Involving Usernames and Passwords**

Incidents involving usernames and passwords that are sent unencrypted and not password protected via email will be entered into DOI CIRC by WO-840 personnel. The Privacy Officer

or NOC DIRM Ops Security is responsible for ensuring the individual sending email is reminded of the prohibition against sending PII or sensitive BLM data via email unencrypted or password protected. The user will need to change the government usernames and passwords compromised by the email. If any administrator usernames/passwords were compromised, the system administrator should be notified to change them. The individual should be required to re-take FISSA+ training. If the FISSA+ training is not accomplished within three (3) business days, then the individual's network access should be restricted. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate. Once all necessary action has been completed inform the WO-840 team so they can close the incident in DOI-CIRC.

#### **4.3.5 Incidents Involving Sensitive BLM Data**

(Financial data, IP addresses, system information, etc.)

Incidents involving sensitive BLM data sent unencrypted and un-password protected via email will be entered into DOI CIRC by WO-840 personnel. The Privacy Officer or NOC DIRM Ops Security for the State or Center owning the network used to send the email has the obligation to ensure the individual sending email is reminded of the prohibition against sending PII or sensitive BLM data via email unencrypted or password protected. The individual should be required to re-take FISSA+ training. If the FISSA+ training is not accomplished within three (3) business days, then the individual's network access should be restricted. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate. Once all necessary action has been completed inform the WO-840 staff to close the incident in DOI-CIRC.

#### **4.3.6 Incidents Involving Lost or Stolen Equipment or Hardcopy Files**

Incidents involving the loss or theft of equipment or hardcopy records should be reported through the BLM Helpdesk. If there is any potential that PII was contained on the missing items that information must be included in the initial report.

### **4.4 BITTF Requirements**

In accordance with the DOI PLMS, when there is a potential breach of PII the Bureau Identity Theft Task Force will meet. The BITTF reports directly to the DOI-CIRC, and evaluates the initial status of the breach. The BITTF is responsible for providing an initial estimate of both the severity of the incident and its potential for harm.

BITTFs must be established when there are incidents that involve an actual breach involving the compromise of PII of more than one individual or if the information was sent to an external BLM address not belonging to the user sending the information. BITTFs may be called in any situation where additional discussion is warranted or beneficial. If a BITTF is required the State or Center Privacy Officer where the incident occurs must schedule a BITTF within 3 business days of the incident. The BITTF should include a conference call option to accommodate geographically separate individuals. The State or Center Privacy Officer will be responsible for ensuring meeting minutes are taken and that WO-840 personnel are kept informed of any updates.

that should be included in the US-CERT notification. BITTFs will be held on a weekly basis until the incident is closed or the BITTF members agree that weekly meetings are no longer necessary.

When a breach occurs, the BLM BITTF is required to respond by:

- Detecting and determining the breach condition for their respective community;
- Immediately notifying DOI-CIRC, the OIG, and other applicable parties, as warranted, of a potential breach;
- Initiating the Department of Interior's Privacy Loss Mitigation Strategy;
- Following ITTF guidance on significant breaches;
- Disseminating ITTF approved and appropriate Public Information and Notifications; and
- Providing support services to aid recovery.

The BITTF must include at a minimum:

- Bureau Privacy Act Officer
- Bureau Chief Information Security Officer
- Representative from WO-840 team
- Representative from the Solicitor's Office
- State/Center Privacy Act Officer
- The NOC DIRM Ops Security
- Management representative for the division where the breach occurred

The following should be invited to the BITTF based on the circumstance of the BITTF:

- Human Resources representative
- Public Affairs representative
- Government Charge Card manager
- Law Enforcement
- Internal Affairs/Inspector General
- The supervisor of the individual suspected of committing the breach

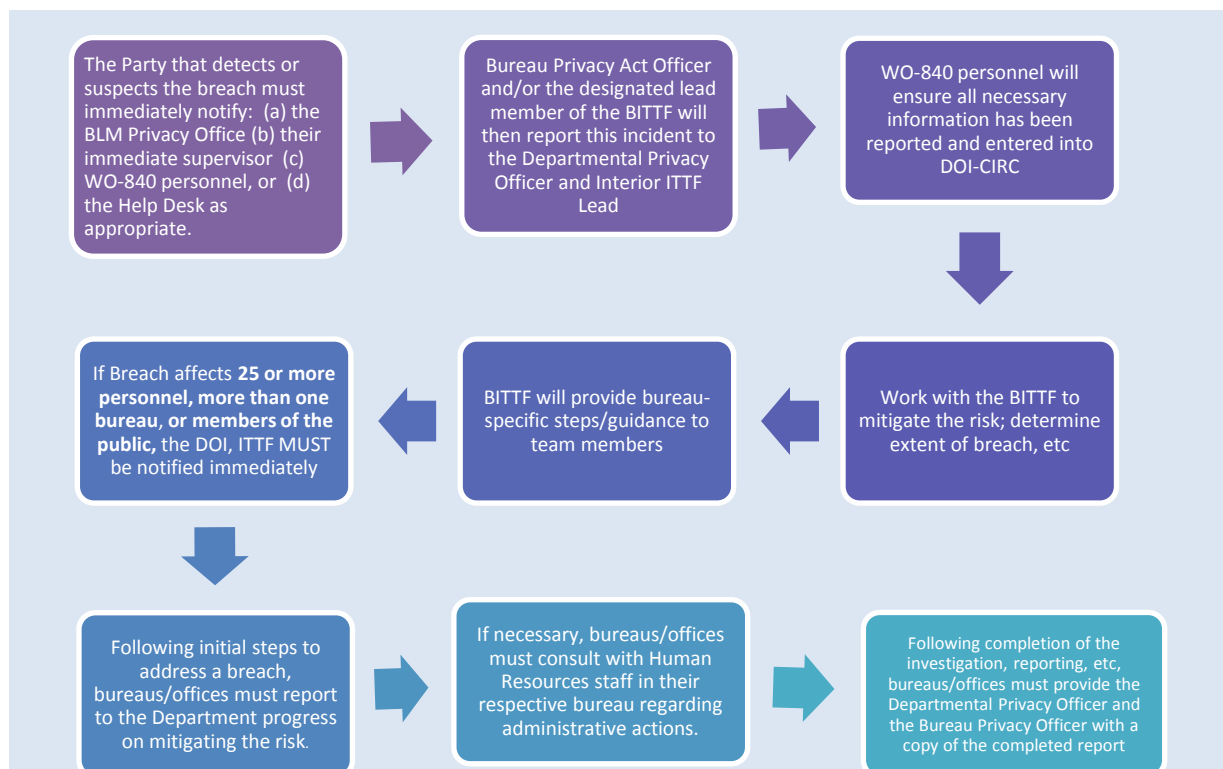
The following individuals will be included in the BITTF at the discretion of the Bureau Privacy Act Officer: Deputy Assistant Director Information Resource Management, DOI Privacy Act Office, and other WO program managers as needed. BITTF's should include a conference call option for geographically separated parties. The State/Center Privacy Officer is responsible for ensuring that BITTF meeting notes are taken and provided to all parties. Additionally, the State/Center Privacy Act Officer is responsible for ensuring that WO-840 team and the Bureau Privacy Act Officer is provided weekly updates using the Standard Breach Reporting Template (Appendix D). BITTFs will be held on a weekly basis until the incident is closed or the BITTF members agree that weekly meetings are no longer necessary.

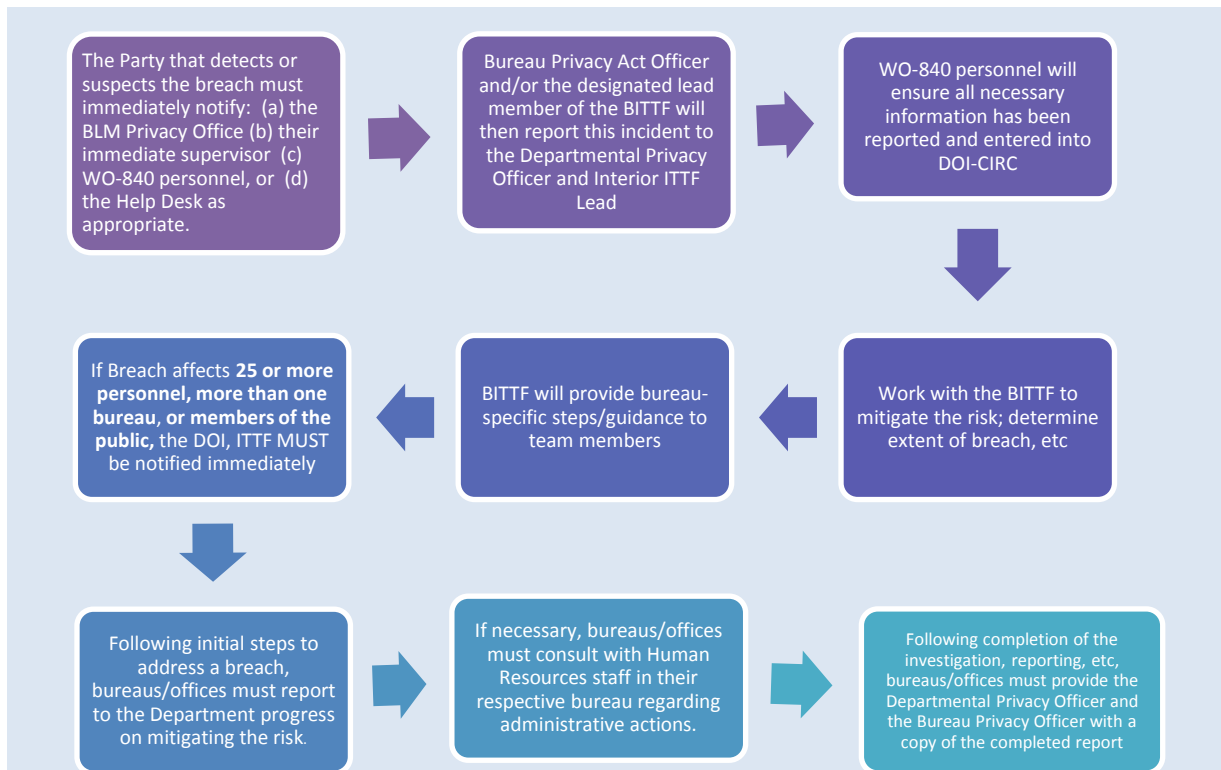
The BITTF agenda will include the following:

- Perform Initial Assessment of the Incident
- Confirm completion of Appropriate Internal Notifications
- Confirm Involvement of Appropriate Personnel
- Determine Exact Nature of Information Loss
- Analyze Information Loss to Determine Potential Impacts

- Determine Mitigation Plan of Action
- Determine External Notification Plan of Action
- Complete Mitigation and External Notification Activities
- Review Lessons Learned

Below are the main activities that must take place when a breach occurs summarized at a high-level in the following graph.





## 4.5 Notification Considerations

Notification letters should not be sent when there is a low potential that the individuals whose information was compromise will suffer any actual harm. The potential for harm is determined by considering:

- Nature of the data elements breached (i.e. social security numbers vs home address only)
- Number of individuals affected (mainly considered in type of notification to use)
- Likelihood the information is accessible and useable
- Likelihood the breach may lead to harm
- Ability of the Agency to mitigate the risk or harm

Credit Monitoring should also only be offered in cases where there is a high potential for harm to the affected individuals. Public affairs should be informed of major incidents so that they can determine whether a press release is needed.

## 4.6 External Breach Notification Policies

Once the BITTF is notified that there is a breach of PII, persons affected by the breach will be notified by the Agency Head or designated senior-level in writing without unreasonable delay,



but no later than ten (10) business days after the determination is made.<sup>4</sup> When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring that any notification and corrective actions are taken.<sup>5</sup>

The following elements that should be considered when determining whether external notification is necessary:

- Nature of the data elements breached (i.e. social security numbers, addresses, home phone number, etc.);
- Number of individuals affected;
- Likelihood the information is accessible and useable;
- Likelihood the breach may lead to harm; and
- Ability of the Agency to mitigate the risk or harm.

Once the Bureau has determined whether an external notification should occur, it must take into consideration the following factors when crafting the external notification:

- Timeliness of the notification;
- Source of the notification;
- Contents of the notification;
- Means of providing the notification; and
- Who receives the notification: public outreach in response to a breach.

Appendix E contains a sample notification letter. An external notification letter must contain the following elements.

---


<sup>4</sup> Notification involving only a limited number of individuals (*e.g.*, under 50) may be also issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy.

<sup>5</sup> The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

## 5.0 HANDLING SPECIAL TYPES OF INCIDENTS

### 5.1 Reporting Unsolicited email (aka SPAM)

If a user is receiving spam:

- Select the message to report.
- Click the spam button  in the toolbar above your message list.
- If the message is open in a separate window, it can be reported as spam by using the same button.
- This will report the message as spam to Google and delete it from the Inbox.
- Alternately, Click the down arrow next to 'Reply', at the top-right of the message pane.
- Select “Report Spam”.

If suspicious email appears to have been sent by someone the recipient knows, but the senders' identity is hidden, this is email spoofing. Malware or dangerous links may be contained in these types of messages. Spoofing should be reported to WO-840 and the following instructions must be followed.

- Retrieve the email headers by clicking on “Show Original” under “More” in the original email message. The header must come from the original email.
- The header information will have a Return-Path: <name@domain> and a Received: from name.domain. See example:
  - Wed, 20 Nov 2013 10:22:13 -0800 (PST)
  - Return-Path: <webmaster@clockmag.ru>
  - Received: from vh2.besthost.by ([2001:67c:2268:1004:4a5b:39ff:fe89:72b1])
  - by mx.google.com with ESMTPS id r8si8088403wjw.9.2013.11.20.10.22.09
- Gmail also has an app to analyze header information:  
<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>.
- Request DOI to have the return path blocked and send the header information.
- If there is a link in the body of the email, request the link be blocked by sending it to [Web\\_filtering@ios.doi.gov](mailto:Web_filtering@ios.doi.gov)
- As a safety precaution, check Splunk logs to ensure user did not follow the link in the email and to confirm that the URL was not accessed by another user. If the user did follow the link, the machine should be scanned and cleaned. Additional monitoring may be necessary to ensure there has been no compromise to the Network.
- If the BLM Network has been compromised the incident needs to be reported to DOI CIRC.

### 5.2 Government Furnished Equipment (GFE)

The BLM requires any loss of Government Furnished Equipment (GFE) containing BLM information electronically stored, such as Smartcards, laptops, Blackberries, flash/thumb drives,

removable hard drives, Personal Digital Assistants, cell phones, or any other type of electronic media to be reported to both the employee's supervisor and the local NOC DIRM Ops Security within one hour of discovery during normal duty hours. The NOC DIRM Ops Security will then follow any published BLM CSIRT procedures and guidance.

### 5.3 Rootkit Incidents

- The machine must be reimaged if a Rootkit has been identified, along with rewriting the Master Boot Record (MBR). Microsoft KB 69013 details fixing and rewriting the MBR:
- <http://support.microsoft.com/kb/69013>
- Performing a disk wipe utility using DBAN or other approved disk wipe utility must be completed before reimaging.

### 5.4 Phishing, Social Engineering Attacks and Hoax Incidents

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent web site that appears legitimate. The email may then ask the user to provide personal information such as account usernames and passwords that can further expose them to future compromises. Additionally, these fraudulent web sites may attempt to infect the user's machine with a virus or other malicious code.

Report suspected and successful phishing or social engineering attempts by:

Messages asking for personal information (phishing)

- Open the message to report.
- Click the down arrow next to 'Reply', at the top-right of the message pane.
- Select 'Report Phishing'.

Additional information regarding phishing and social engineering attacks may be found at:

- Avoiding Social Engineering and Phishing Attacks  
<http://www.us-cert.gov/cas/tips/ST04-014.html>
- Protecting Your Privacy  
<http://www.us-cert.gov/cas/tips/ST04-013.html>
- Recognizing and Avoiding E-mail Scams  
[http://www.us-cert.gov/reading\\_room/emailscams\\_0905.pdf](http://www.us-cert.gov/reading_room/emailscams_0905.pdf)
- Get assistance if fallen prey to an attack and take proactive measures to protect financial data and identity information. Follow the steps outlined above to report the breach to WO-840 personnel and consider following the steps outlined on the Federal Trade Commission's Identity Theft Website:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

## 6.0 ROLES AND RESPONSIBILITIES

The primary function of any Incident Response Team formed during an IT security incident is to prevent or minimize damage to the confidentiality, integrity and availability of BLM data, and to expedite a speedy recovery to normal operations and a secure environment.

Each organizational unit within the Bureau is required to have some level of incident response capability and will generally have differing resources available. The roles and responsibilities of IT Security personnel as they relate to Incident Response are described below.

### 6.1 BLM Computer Security Incident Response Team (BLM-CSIRT)

IT Security and Incident Response personnel represent the core of the response and recovery efforts. BLM-CSIRT members are from the WO-840 IT Security Division and the NOC DIRM Operational Security Branch. These team members are responsible for investigating, documenting, and formally reporting any actual or perceived security incidents to DOI and/or US-CERT. IT Security and BLM CSIRT personnel are also responsible for:

- Being available for contact by anyone who discovers or suspects that an incident involving the organization has occurred.
- Performing initial incident response.
- Analyzing incident data and determining the potential impact of the incident.
- Acting appropriately to limit damage to the organization and restore normal services.
- Gathering evidence for forensic analysis.
- Assisting with incident policy development and incident response education.
- Performing post-incident compliance, restoration, and vulnerability testing.
- Providing accurate incident information to key decision-makers.
- The BLM CSIRT will coordinate response activities that have been escalated or reported by NOC DIRM Ops Security. Depending upon the severity, this may require the formation of a formal incident response team with members from other subject areas such as Law Enforcement, Human Resources, or the Solicitor's Office.
- Responsible for ensuring the incident is reported to DOI-CIRC

The BLM CSIRT receives reports of IT security incidents and is responsible for the plan of action to address the IT security incident. Centralization of the response activity facilitates reporting to the Department and tracking of incident types occurring in the Bureau.

The core members of this team are located in Lakewood, Colorado. The contact information is:

- Email: BLM\_INCIDENTS\_IT\_SECURITY
- BLM IT Security Phone number: 303-236-0611(rings at all desks)

### 6.2 End User Responsibilities

All end-users of BLM systems, whether federal employees or government contractors are required to immediately report potential, suspected or confirmed reportable security incidents (defined in section 2.4) and any system anomalies. They are also expected to give their full

cooperation to the Incident Response Team during an IT security incident. Reporting should be to the National Help Desk or to BLM\_INCIDENTS\_IT\_SECURITY email.

All users of Federal IT resources are accountable for all activity performed under their unique user ID.

### **6.3 Assistant Director, Information Resource Management (ADIR-IRM)**

The ADIR-IRM is responsible for establishing and implementing the policies relating to the overall Information Technology program. As part of that responsibility, the ADIR budgets for the protection of BLM's information assets and directs the development and enforcement of policies in this area. Computer Security Incident Response is a critical service necessary for the protection of the bureau's information assets.

The ADIR-IRM engages key senior management officials and system owners in the event of a serious incident and making system shut-down decisions when necessary.

### **6.4 The Bureau Chief Information Security Officer (BCISO)**

The Bureau Chief Information Security Officer (BCISO) is responsible for establishing and implementing the information security policies for responding to the detection of adverse events and assuring that appropriate action is taken to minimize the consequences of such events.

This official has the following responsibilities relating to the CSIRT and the overall incident response capability:

- Developing and disseminating information concerning the potential dangers of computer security incidents, guidelines for its control, and reporting of incidents.
- Notifying the ADIR-IRM and bureau management of computer security incidents.
- Notifying DOI-CIRC and other appropriate Departmental and federal officials of applicable computer security incidents.
- Assuring that appropriate action is taken to minimize the consequences of each adverse event.
- Developing and issuing instructions for detection and removal of malicious software.
- Coordinating with OIG and Human Resources for guidance in determining what constitutes criminal intent and employee misconduct.

### **6.5 Incident Response Manager**

The Incident Response Manager manages the overall response and recovery activities for all security incidents, deciding the severity level of each incident and assigning staff members to perform response and recovery tasks accordingly.

The Incident Response Manager performs the following tasks:

- Oversees the operation of the incident response process.
- Communicates and coordinates with the ADIR-IRM and/or BCISO on incident notification, severity levels, and status.
- Coordinates response and recovery activities with other divisions of the bureau as needed to acquire additional physical or human resources.

- Communication and coordination with DOI-CIRC, US-CERT or the OIG for detailed response and recovery activities, as required.
- Consults with the ADIR-IRM, BCISO, DOI-CIRC, or OIG regarding decisions to pursue legal action and gather evidence, or quickly react to protect affected systems and return operations to normal as quickly as possible.
- Manages, directs and assigns Ad Hoc Incident Response Team members when special expertise or advice is required.

## **6.6 NOC DIRM Operational Security**

NOC DIRM Operational Security is responsible for assisting in reporting and resolving identified IT Security incidents. This includes disseminating guidance, educating end users and providing assistance and guidance during an IT security incident. They ensure that Bureau policies are followed for resolving IT security incidents.

- Educating computer users to report confirmed or suspected computer security incidents to the National Help Desk, or consult immediately with the NOC DIRM Ops Security for advice on how to report it.
- NOC DIRM Ops Security reports all incidents to the BLM CSIRT. Any incidents handled locally should be reported by submitting an Incident Report to the BLM CSIRT.

## **6.7 Technical Support Subject Matter Experts**

Systems, Network and Database Administrators play critical roles in incident handling. They will likely be assigned by the Incident Manager to the Incident Response Team through the NOC DIRM Operational Security as needed.

- Systems Administrators are generally responsible for establishing and maintaining user access to systems and components, in addition to performing various other functions to support the administration of the system. They will assist with resolution of IT security incidents as directed by the Incident Manager or BLM CSIRT.
- Network Administrators have knowledge of the network, its configuration, and interface components. Detailed understanding of the compromised component's location and its relationship to the network or other connections is critical to understanding and resolving an incident.
- Database administrators must evaluate whether changes have been made to the database structure or configuration and determine whether any database-specific programs (e.g., stored procedures or queries) have been modified.

Described below are the general responsibilities for Technical Support Subject Matter Experts during the incident response process. The specific responsibilities for each system or application will vary, but must be identified and defined to BLM IT Security WO-840 during Pre-incident Planning:

- Actively participate, as assigned, as members of the Incident Response Team and provide subject matter expertise.
- Preserve and protect the evidence compiled as a result of the investigation or research, ensuring that forensic evidence is maintained.

- Ensure all evidence is provided to the appointed Evidence Custodian, in accordance with established evidence Response requirements and procedures.
- Rebuild or participate in the rebuilding of compromised systems. In cooperation with the Technical Lead, take action to effectively assess, contain, and recover from all IT security incidents; examine compromised systems to identify changes; and remove all unauthorized code and software from the compromised system.
- Ensure that compromised systems are kept off-line from the network and/or disconnected from the Internet as appropriate until it has been determined how the intrusion occurred and the vulnerabilities that allowed the compromise have been corrected.
- Assist the Technical Lead in any research or investigation required to determine the extent of any damage done or the impact of the IT security incident on the system(s) administered.
- Load all necessary system patches and authorized application software, as identified by the system administrator.
- Verify all user accounts and system privileges prior to reloading any software or services.
- Recover data using a trusted backup, i.e., a backup that has not been compromised, of the operating system.
- Ensure the affected system is ready for secure operation by confirming that the root causes of the incident have been identified and mitigated.

## **6.8 Physical Security/Facilities Management**

Provides guidance and assistance when computer security incidents involve breaches of physical security or unauthorized access into secured physical areas, or when assistance is needed for securing of physical area as part of an incident investigation.

## **6.9 IT Investigative/Forensics Expert**

Depending on the severity of an incident, or if a criminal investigation results as part of the incident, an IT Investigative/Forensics expert may be required. The Incident Response Team Manager must authorize the collection of any evidence. This manager will contact the local OIG or the DOI-CIRC before authorizing the gathering of evidence and follow any specific instructions they may provide. When appropriate, System Owner, BCISO, DIRM Division Chief or OIG liaison will be consulted before collection of evidence takes place.

## **6.10 Evidence Custodian**

As a general rule, the fewer people that handle evidence, the greater its admissibility in a court of law. For this reason, an Evidence Custodian is needed on the Incident Response Team when a criminal investigation may be involved. This individual would be charged with gathering, handling, storing and documenting evidence and managing the chain of custody, although other group members will also be gathering, handling, and copying evidence in the course of incident handling. The Evidence Custodian would facilitate evidence handling and serve as a single point-of-contact for legal, law enforcement, BLM, and DOI personnel in all matters relating to evidence.

### **6.11 Legal Liaison**

The Department of the Interior's (DOI) Office of Inspector General (OIG) serves as the Incident Response Team's Legal Liaison, responsible for providing direction and guidance to ensure the team follows proper legal procedure while investigating the incident.

### **6.12 Public Affairs/Media Relations**

When IT security incidents have a direct bearing on the public or when incidents become public knowledge, it may become necessary to issue a statement. The Public Affairs Officer (PAO) is usually the organization's sole point-of-contact with the media when it releases information. Statements sent to the Public Affairs Officer are to first be cleared with the Incident Response Team Manager and BCISO before release to the public. The Bureau will use the PAO for the Washington Office or the PAO for the state affected by an incident, as appropriate.

The scope of responsibilities and rules for release of information may vary significantly depending on the type, severity and timing of an incident. Specific rules of release must be established and agreed upon prior to enacting this role on the team.

### **6.13 Human Resources**

A human resource representative or point-of-contact will be included on the team, as necessary, to help ensure that the team does not violate employees' rights (e.g., privacy) during any investigation and provides guidance on appropriate disciplinary measures in the event an employee is found to be materially involved in the incident.

### **6.14 Privacy Office**

Provides guidance for personal information (PII) and other privacy-related concerns during incident handling. PII breaches and incidents must be escalated to the Privacy Office.

### **6.15 System Owner**

System owners have intimate knowledge of the criticality of the system to the organization's mission and therefore have the following team responsibilities:

- Deciding whether to isolate affected systems or shut them down.
- Deciding whether a backup system must be put into operation immediately or the system can be kept down until the main system is validated and any system vulnerabilities corrected.
- Analyzing the data to ensure proper format and output.



## **7.0 REGULAR PLANNING / PREPARATION**

Successful recovery from an incident requires having had thorough planning and preparation before the incident occurred. Each incident response phase depends, in some way, on adequate preparation. Examples of required preparation include:

- An in-place and fully functioning Configuration/Change Management Process
- Documented test procedures for systems that may have to be restored or rebuilt during the recovery phase
- Pre-arranged and tested out-of-band communication channels
- Complete and tested Contingency Plan for each IT system
- Current contact lists for internal and external resources
- An identified and trained Incident Response Team

Adequate preparation can mean the difference between recovering an affected system to normal operational status in a short period of time, with minimal data loss, by using reliable, tested backups and a catastrophic loss of data because backup tapes are corrupted or contaminated.

A detailed outline of Planning / Preparation follows.

### **7.1 Define a baseline for all systems**

A baseline is necessary to identify changes made to the system(s) by the incident and to use for reference in the event that rebuilding the system becomes necessary. Baseline change management processes must be in place and being utilized to ensure all changes are included.

- Develop systems baseline documentation.
- Use change management processes for all systems

### **7.2 Perform regular back-ups of data and software**

Routinely backup data and system software. Data should be backed up at a frequency and using methods that will meet information owner's requirements and support a recovery plan suitable for the business process supported by the data. System and application software should be backed up following upgrades. Follow BLM Policy and Standards.

Back-up media should routinely be tested for reliability and accuracy. Maintaining accurate and up-to-date records of backups, including tracking back-up media attributes (e.g. identifiers, age, location, backup session dates, etc.) can prove invaluable when analyzing whether or not a particular back-up set is likely to be reliable and uncontaminated.

### **7.3 Develop and document test procedures for each system**

Test procedure documentation can be used to test for possible intrusions and to determine if systems have been restored completely after an intrusion.

### **7.4 Incident Handling Tools**

Incident detection and handling tools are used by the Incident Response Team to investigate the incident, gather information and determine root cause.

The following are some of the tools and/or resources available for Incident Response investigation.

Type of Incident or usage	Tool (update list)
Antivirus/malware/spyware	Symantec
Internet attack	Barracuda, Splunk
Log file examination, web monitoring	Splunk
Trojan/malware on machine	Symantec, McAfee Vulnerability Manager
Web site misuse	BlueCoat
Packet capture	Wireshark
Web site vulnerabilities	McAfee Vulnerability Manager
SPAM, phishing, DOS	Bison Connect
Machine names, IPs	Active Directory (AD)
Data loss prevention	Symantec DLP
Host names to IP	DHCP logs
VPN use	Juniper

## **8.0 INCIDENT RESPONSE TRAINING, TESTING AND EXERCISES**

### **8.1 Incident Response Training**

Training for Incident Response is contained in other documents or in DOILEARN, in support of NIST SP 800-53 Rev 4 IR controls. Most information is tool specific and found in vendor materials, vendor web sites or in local SOPs.

### **8.2 Incident Response Testing and Exercises**

Incident Response procedures must be tested annually to meet NIST SP 800-53 Rev 3 controls. Tests may be Table Top Exercises (TTX), scheduled incident handling, testing, and also unannounced scheduled incident handling. An After Action report should follow the test documenting the results, lessons learned and attendees. This may be combined with Contingency Planning (CP) tests.

### **8.3 Incident Handling Scenarios**

NIST has developed Incident Handling Scenarios and has “strongly encouraged organizations to adapt these questions and scenarios for use in their own incident response exercises.” For additional information or to implement additional Incident Handling exercises and tests, see NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, which is available at <http://csrc.nist.gov/publications/PubsSPs.html>.

Exercises involving incident handling scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes. The incident response team or individual team members are presented with a brief scenario and a list of questions related to the scenario. The team then discusses each question and determines the most likely answer.

The goal is to determine what the team would really do and to compare that with policies, procedures, and recommended practices to identify any discrepancies or deficiencies. For example, the answer to one question may indicate that the response would be delayed because the team lacks a particular piece of software or because another team within BLM or the Department does not provide off-hours support.

### **8.4 Additional Incident Response Resources**

In support of NIST SP 800-53 Rev 4, NOC DIRM Ops Security serves as the first point of contact for BLM. The BLM CSIRT is available for questions and guidance.

Many useful websites provide information about IT security incidents and incident response. Incident Response Teams can reference both federal and commercial incident response websites in order to keep up with the latest threats and solutions to security incidents.

The U.S. Computer Emergency Readiness Team (US-CERT) <http://www.us-cert.gov> is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). They have a central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government.

The National Institute for Standards and Technology (NIST) provides a searchable index of computer vulnerabilities with their development of the National Vulnerability Database (NVD). NVD is the U.S. government repository of standards based vulnerability management data

represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

The Forum of Incident Response and Security Teams (FIRST) <http://www.first.org/>, established by a number of government and private sector organizations, brings together a variety of computer security incident response teams from government, commercial, and academic organizations to assist in eradication of incidents, and promote the sharing of information among members and the community at large.

The Internet Storm Center (<http://isc.sans.org/>) was established to provide a free, centralized repository of Internet security firewall intrusions. The storm center maintains up-to-date intrusion activity information and uses the data it collects for trend analysis and reporting; this helps the Internet community to prioritize security measures and take pre-emptive action to reduce the spread of focused attacks.

US Computer Emergency Readiness Team (US-CERT)	<a href="http://www.us-cert.gov">http://www.us-cert.gov</a>
BLM IT Security	<a href="http://teamspace/sites/blimits/Page/Home.aspx">http://teamspace/sites/blimits/Page/Home.aspx</a>
NIST Computer Security Division	<a href="http://csrc.nist.gov/groups/SMA/fisma/overview.html">http://csrc.nist.gov/groups/SMA/fisma/overview.html</a>
U.S. Department of Homeland Security	<a href="http://www.dhs.gov">http://www.dhs.gov</a>
National Vulnerability Database	<a href="http://nvd.nist.gov">http://nvd.nist.gov</a>
US-CERT Incident Reporting System	<a href="https://forms.us-cert.gov/report">https://forms.us-cert.gov/report</a>
Forum of Incident Response and Security Teams (FIRST)	<a href="http://www.first.org">http://www.first.org</a>
SANS Institute	<a href="http://www.sans.org">www.sans.org</a>
SANS Internet Storm Center	<a href="http://isc.sans.org">http://isc.sans.org</a>
Carnegie Mellon CERT	<a href="http://www.cert.org/">http://www.cert.org/</a>

## 9.0 EVIDENCE HANDLING

### 9.1 Authorization

Incident Handling Group members are not responsible for conducting forensic examinations. They are responsible for providing assistance in gathering evidence that could be used in law enforcement investigations. Team members must be trained in gathering evidence and they must follow appropriate evidence handling procedures. The Incident Management Coordinator must authorize the collection of any evidence.

Contact the local Office of the Inspector General (OIG) or the Department CSIRT before gathering any evidence. Follow any specific instructions they may provide.

### 9.2 Emergencies

In some cases, it may not be possible to contact the OIG or other appropriate officials and the evidence may be in jeopardy. If this is the case, the priority is to isolate the computer system as described in Phase 4: *Contain the Incident*, and restrict access to the computer.

### 9.3 Gathering Evidence

Gather evidence in such a way that it is not altered and the chain-of-custody is maintained and minimized. Document everything so that it is possible to recreate the exact steps that were followed to collect the evidence. RFC-3227 provides a good overview of the best practices.

### 9.4 Chain-of-Custody

The chain-of-custody is a log that contains the locations, times, dates, names and signatures of the people who had custody of an evidence item. The log is referred to as a chain-of-custody form.

The original copy stays with the evidence item. Keep a copy when the item is transferred to law enforcement.

### 9.5 Marking Evidence

Evidence tape is used to show that an item of evidence has been accessed. The tape is applied in such a way that it breaks when the item is accessed. For example, evidence tape can be attached across the back of the computer and the computer case. If the case is opened, the evidence tape will break. The tape is signed to ensure that it is the original piece of tape.

A mark should be placed on the item so that it is possible to identify the device, if the evidence tags are removed. Usually, initials can be written on the item in a discreet place. For example, the initials of the person collecting the evidence can be written on the back of the computer or on top of the hard drive.

### 9.6 Incident Records Retention and Destruction

General Records Schedule (GRS) 24, Information Technology Operations and Management Records, specifies that "computer security incident handling, reporting and follow-up records" should be destroyed "3 years after all necessary follow-up actions have been completed." More specifics of what needs to be retained include: "Computer Security Incident Handling, Reporting and Follow-up Records. Destroy/delete 3 years after all necessary follow-up actions have been completed. Reports and documentation of Web site defacement; Hacks; Break-in records; Improper usage by staff; Misuse of system; Security breaches; Security break-ins; Security failures; Unauthorized intrusions; Virus threats."

All documents and incident evidence must be securely stored in a location with limited access.

Pursuant to the aforementioned guidance, all Incident Records shall be destroyed by approved destruction methods (i.e.: Approved paper and disk shredders, approved disk wipers, etc.) three years after all necessary follow-up tasks have been completed.

### **9.7 Collecting Procedures**

Ideally, the entire computer should be collected. It is not necessary to send the monitor or keyboard. In some cases, the OIG may require additional equipment such as a scanner, tape drive, etc. At a minimum, the hard drive can be removed from the PC.

Do not do anything on the victimized system that would change its state of configuration, system logs, etc. With this rule in mind, the following procedures should be used:

1. Document everything in a non-spiral bound notebook and number the pages.
2. List the systems involved.
3. List people involved.
4. Document cable connections (photographs can simplify this step).
5. Document screen contents (photograph, or perform screen prints when possible).
6. Document network connections (ifconfig on UNIX, ipconfig on Windows.)
7. Document the difference between system time and the 'real' time.
8. Shut down the system using the appropriate commands.
9. Remove the hard drive, if the whole system is not seized.
10. Seal the hard drive in an envelope or box (use antistatic material).
11. Seal the container with evidence tape. If the whole computer is seized, apply the evidence tape to the case in such a way that it cannot be opened without detection.
12. Sign the evidence tape.
13. Attach an identification tag that identifies the item, date, time and collector. Document the item in the notes.
14. Maintain custody of the hard drive, system, or device (keep it in a safe, a locked drawer, etc.).
15. Send the hard drive, system, or device to the forensic examiner as directed. Use a chain-of-custody form to transfer the hard drive to the forensic examiner.
16. Do not conduct any examinations on the original evidence.
17. Do not use any tools that could write to the hard drive in any way.

## **9.8 Evidence Gathering Materials**

Materials to have on hand include:

- Notebook (non-spiral bound) and Pen (not pencil)
- Camera (for documenting connections and photographing the screen)
- Evidence tape
- Permanent marker (to sign evidence tape)
- Chain-of-custody forms
- Evidence Tags
- Shipping container (for entire computer)
- Anti-static bags (for hard drive)
- Tools (#2 Phillips screw driver, needle nose pliers, etc.)

### **9.8.1 Law Enforcement**

In some cases, where laws have been broken, or where there was criminal intent, an incident may require the involvement of law enforcement. The threat level of these incidents is 'Critical' and requires immediate attention. Take the following actions as soon as possible:

- Contact the supervisor
- Contain the system
- Contact the Office of the Inspector General (OIG) for guidance
- Follow the instructions of the OIG
- Contact the Bureau Incident Management Coordinator or US-CERT

In some cases, steps may need to be taken to preserve the evidence.

### **9.8.2 Reports and Information**

#### **Statistical Reports**

The BCISO will provide statistical reports that show the number of incidents per category over time. These reports can be used to help determine future computer system hardening strategies and priorities. Detailed report information that will be provided to the general computer security incident response community will be sanitized to remove specific details about individuals.

#### **Marking of Reports**

All reports that contain incident details will be marked as 'For Official Use Only' or 'Sensitive But Unclassified.' Reports will be disseminated to those with a need to know.

## 10.0 EXTERNAL CONTACTS

### Media Contacts

Contact the appropriate public affairs office, if an incident has a possibility of generating public interest. All callers should be referred to the BLM Office of Public Affairs. They may be contacted at 202-452-5125.

### If a Reporter Contacts You:

- Get their contact information. Politely explain that you are not authorized to release any information and that you will pass their information request along your public affairs office.
- Contact your supervisor.
- If this involves an incident with a high threat level, contact the Incident Manager, BLM CSIRT manager or the BCISO.
- Contact your public affairs office and brief them on the incident. Give them the reporter's contact information.

In some cases, you may be authorized or directed to talk with reporters. If this happens, remember the following:

- State only the facts and stick to the subject.
- If you don't know the answer, say so.
- Do not offer opinions.
- Keep your answers short.
- Be polite.
- Remember that you are representing the Bureau, the Department, and the Government.
- Get the reporter's contact information so you can provide follow up information.

### 10.1 Information Sharing with Outside Parties

DOI encourages cooperation between the bureaus in any security activities, as this fosters trust and community among security personnel in all bureaus. Good relationships and information sharing between bureaus increases protection and security across the entire Department. This is especially true with incident response. Should a person be contacted either by another bureau's CSIRT or security personnel for assistance with an incident that they are responding to, be understanding of the circumstances and cooperate as much as possible. If a person is uncomfortable with the circumstances or sensitivity of information involved in this cooperation, ask for facilitation from DOI-CIRC.

If you are contacted directly by DOI- CIRC or by the OIG for assistance or information related to incident response, you are expected to cooperate and communicate fully.

There are instances where it may be appropriate to exchange Security Incident information with outside parties, such as other government non-DOI agencies, software vendors, security appliance vendors, external ISPs, owners of attacking IP addresses, and the like.



Communications regarding on-going incidents with non-BLM or DOI organizations must be coordinated and approved through the BLM CSIRT. Metrics

## **10.2 Requests**

Requests may be made to WO-840 who will in turn request information from DOI-CIRC if necessary. A yearly report is published.

## 11.0 ACRONYMS

The following table contains acronyms used within this document:

ACRONYM	MEANING
<b>BITTF</b>	Bureau Identity Theft Task Force
<b>BCISO</b>	Bureau Chief Information Security Officer
<b>BCSIRT</b>	Bureau Computer Security Incident Response Team
<b>CDROM</b>	Compact Disk Read Only Memory
<b>CIO</b>	Chief Information Officer
<b>CSIRT</b>	Computer Security Incident Response Teams
<b>ESP</b>	Enterprise Services Portal (could also include DOICIRC)
<b>DIRM</b>	Division of Information Resources Management
<b>DOI</b>	Department of the Interior
<b>DOICIRC</b>	Department of the Interior Computer Incident Response Capability
<b>DoS</b>	Denial of Service
<b>DNS</b>	Domain Name Server
<b>FISMA</b>	Federal Information Security Management Act
<b>IA</b>	Information Assurance
<b>IDS</b>	Intrusion detection system
<b>IT</b>	Information Technology
<b>NIDS</b>	Network Intrusion Detection System
<b>NOC</b>	National Operations Center
<b>OIG</b>	Office of the Inspector General
<b>OMB</b>	Office of Management and Budget
<b>PII</b>	Personally Identifiable Information
<b>PGP</b>	Pretty Good Privacy
<b>POC</b>	Point of Contact
<b>US-CERT</b>	United States Computer Emergency Readiness Team

## **APPENDIX A: QUICK REFERENCE ON SAFEGUARDING PII, BREACH MITIGATION AND INCIDENT MANAGEMENT**

The federal government and DOI have established policies and procedures to appropriately handle and safeguard PII, as well as respond to and mitigate PII losses and security incidents.

### **Federal Guidance:**

**OMB 06-15, *Safeguarding Personally Identifiable Information*:** This Memorandum outlines the responsibility of agencies to safeguard PII and provide training to employees that access or handle PII. OMB 06-15 also directs agencies to conduct reviews of policies and processes and take corrective action as appropriate to prevent the intentional or negligent misuse of, or unauthorized access to, PII. Full text of 06-15 may be accessed via <http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf>.

**OMB 06-19, *Reporting Incident Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*:** This Memorandum revised incident reporting requirements, stipulating that agencies report all incidents involving PII within one hour of discovering the incident to US-CERT located within the Department of Homeland Security. Full text of 06-19 may be accessed via <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf>.

**OMB 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*:** This Memorandum is a consolidation of the 05 and 06 series memoranda to ensure implementation of all previous recommendations. OMB 07-16 provides guidance to agencies on the: development of a breach response team; routine for the periodic review of PII; review, reduction, or elimination, of the unnecessary use of social security numbers; and corrective actions. Full text of 07-16 may be accessed via <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>.

**OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*:** This Memorandum requires agencies to implement the recommendations outlined in the President's Identity Theft Task Force, such as the identification of a Core Response Group (CRG) that will be convened upon identification of a potential data breach. The CRG should include agency senior leadership such as the Chief Information Officer (CIO), Inspector General (IG), Chief Privacy Officer (CPO), and Inspector General (IG). Agencies must develop a risk-based analysis to determine whether an incident is vulnerable to identity theft. Agencies must also develop a response plan to identify mitigation measures and notify affected individuals. Full text of the Memorandum may be accessed via [http://www.dod.mil/pubs/foi/privacy/OMB\\_20Sept2006.pdf](http://www.dod.mil/pubs/foi/privacy/OMB_20Sept2006.pdf).

**OMB Circular A-130, Appendix I: *Federal Agency Responsibilities for Maintaining Records About Individuals*:** [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_i.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html).

**President's Identity Theft Task Force, *A Strategic Plan*:** <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

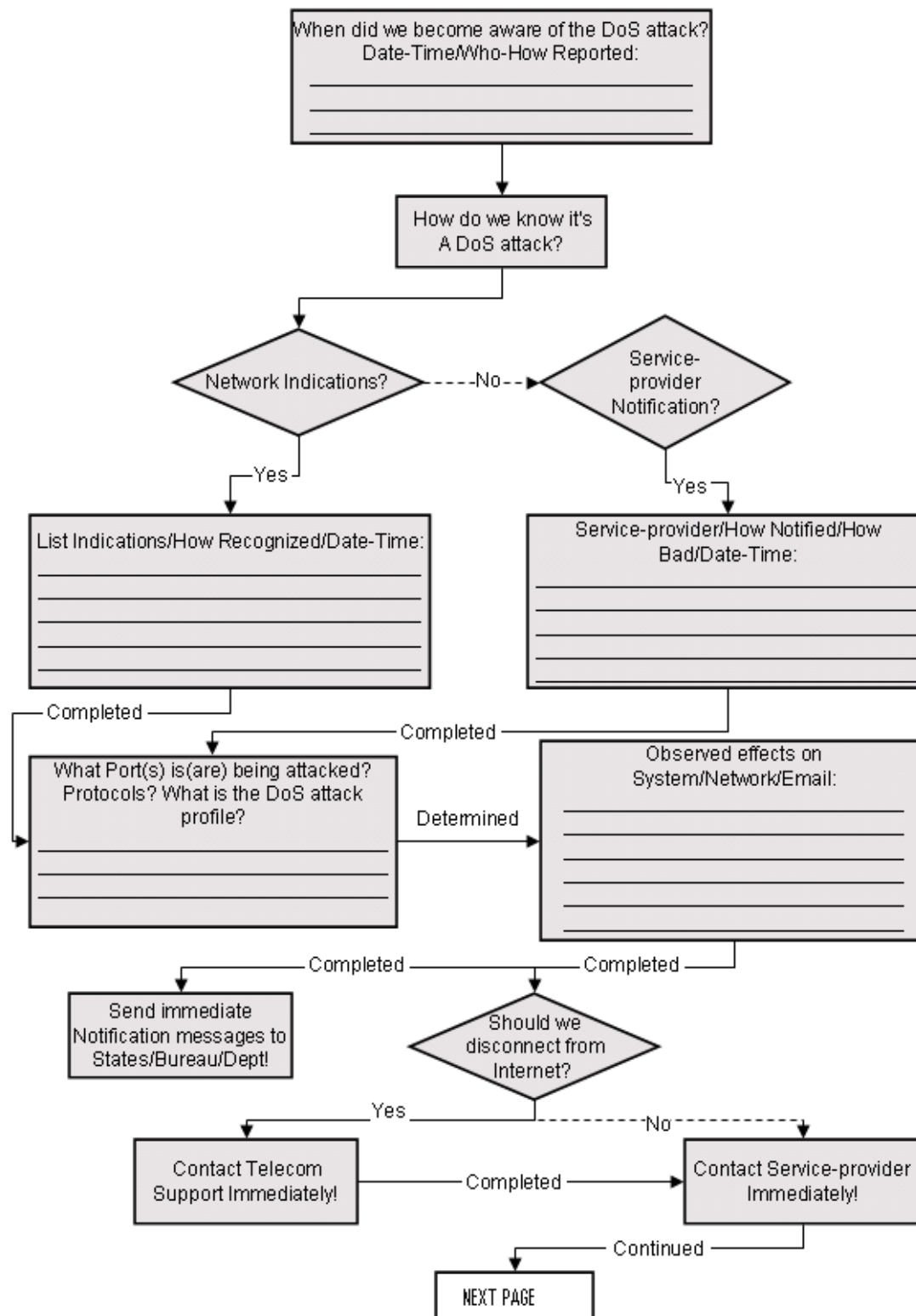
DOI Policies and Directives:

**Department of Interior Privacy Loss Mitigation Strategy (Version 1):** The PLMS is the overall policy framework for the development and/or implementation of an incident management/breach response policy, ID Theft Task Force, Information Reduction Team, policies and procedures to safeguard PII, and SSN reduction strategy. Each Bureau and Office is expected to develop a PLMS based on the DOI framework.

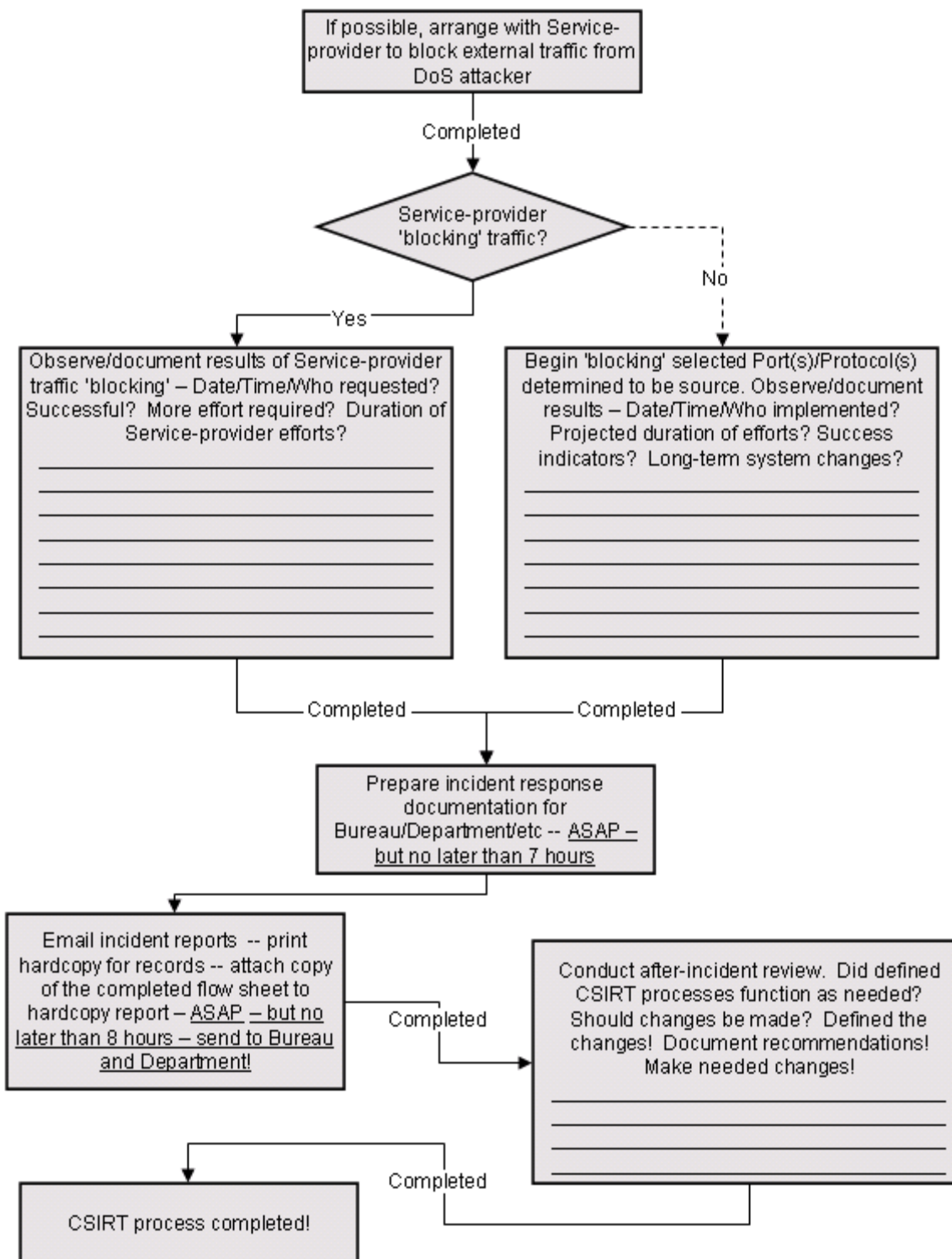
**Departmental Privacy Act Manual, Section 383 DM 4.7****IRM Bulletin 2001-004, *Protecting Sensitive Data when transferring Donating or Disposing of Computer Equipment***

**OCIO Directive 2006-016, *Office of Management and Budget Requirements for Safeguarding Personally Identifiable Information (June 15, 2006)*:** This memo outlines how OMB guidance on safeguarding PII should be implemented throughout all DOI Bureaus and Offices. Full text of the memo may be accessed via <http://www.myinterior.doi.net/ocio/imd/privacy/2006-016%20OMB%20Requirements%20for%20Safeguarding%20Personally%20Identifiable%20Information.pdf>.

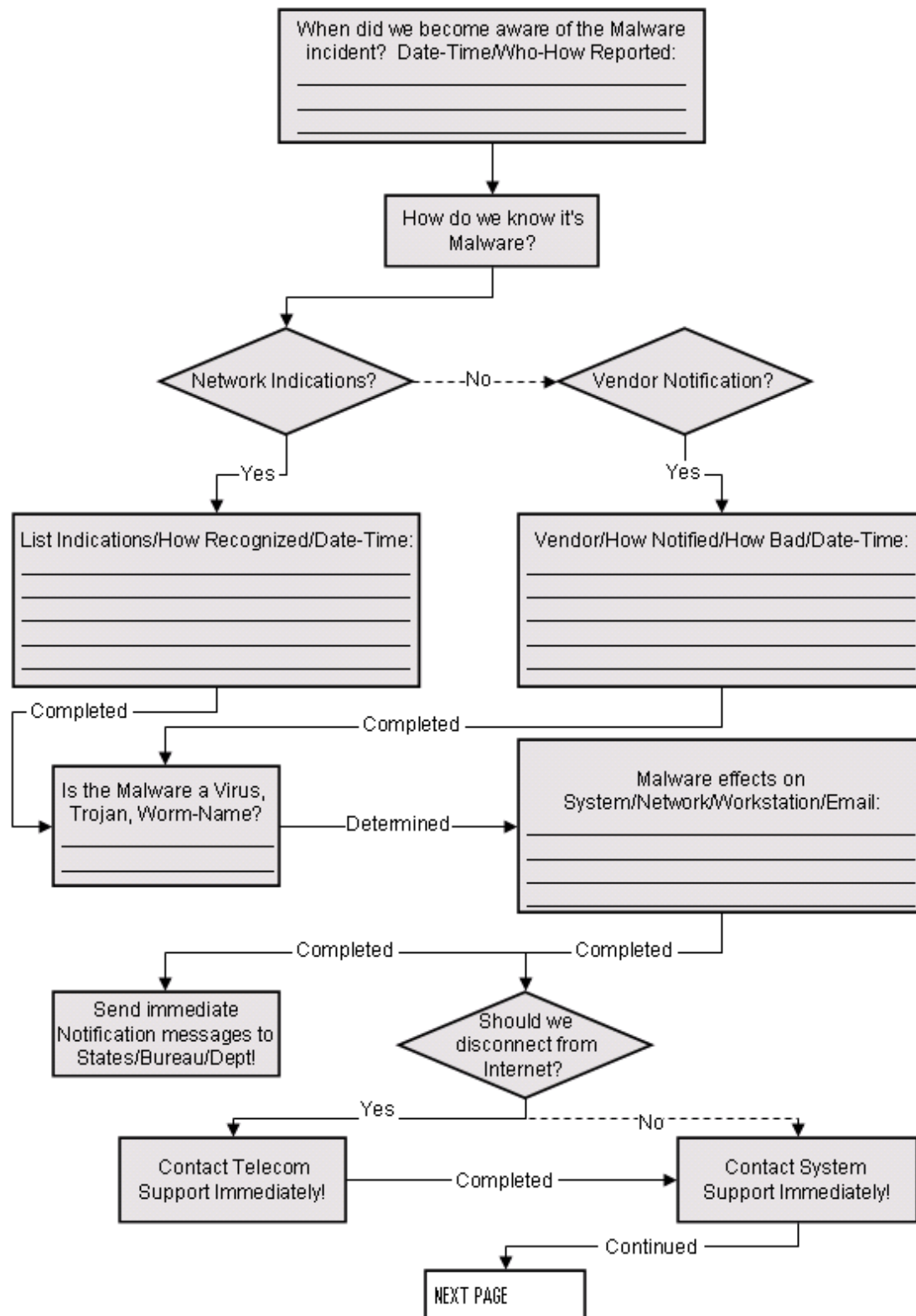
**DOI Secretarial Memorandum, *Important Notice on Safeguarding Personally Identifiable Information* (June 20, 2006)**

**APPENDIX B: INCIDENT FLOW CHARTS****Denial of Service (DoS) Attack Flowchart**

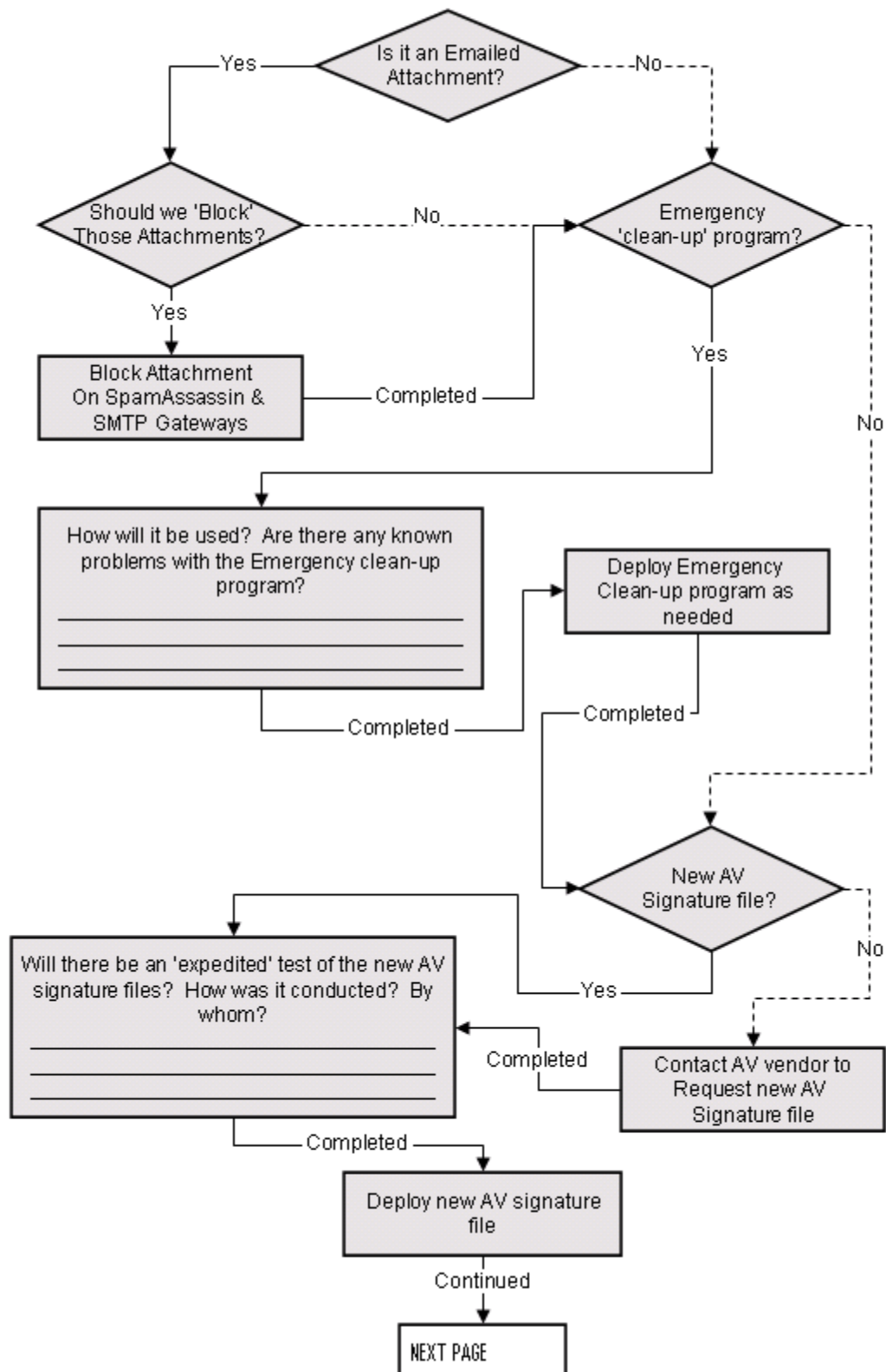
## Denial of Service (DoS) Attack Flowchart



## CSIRT Malware Flowchart

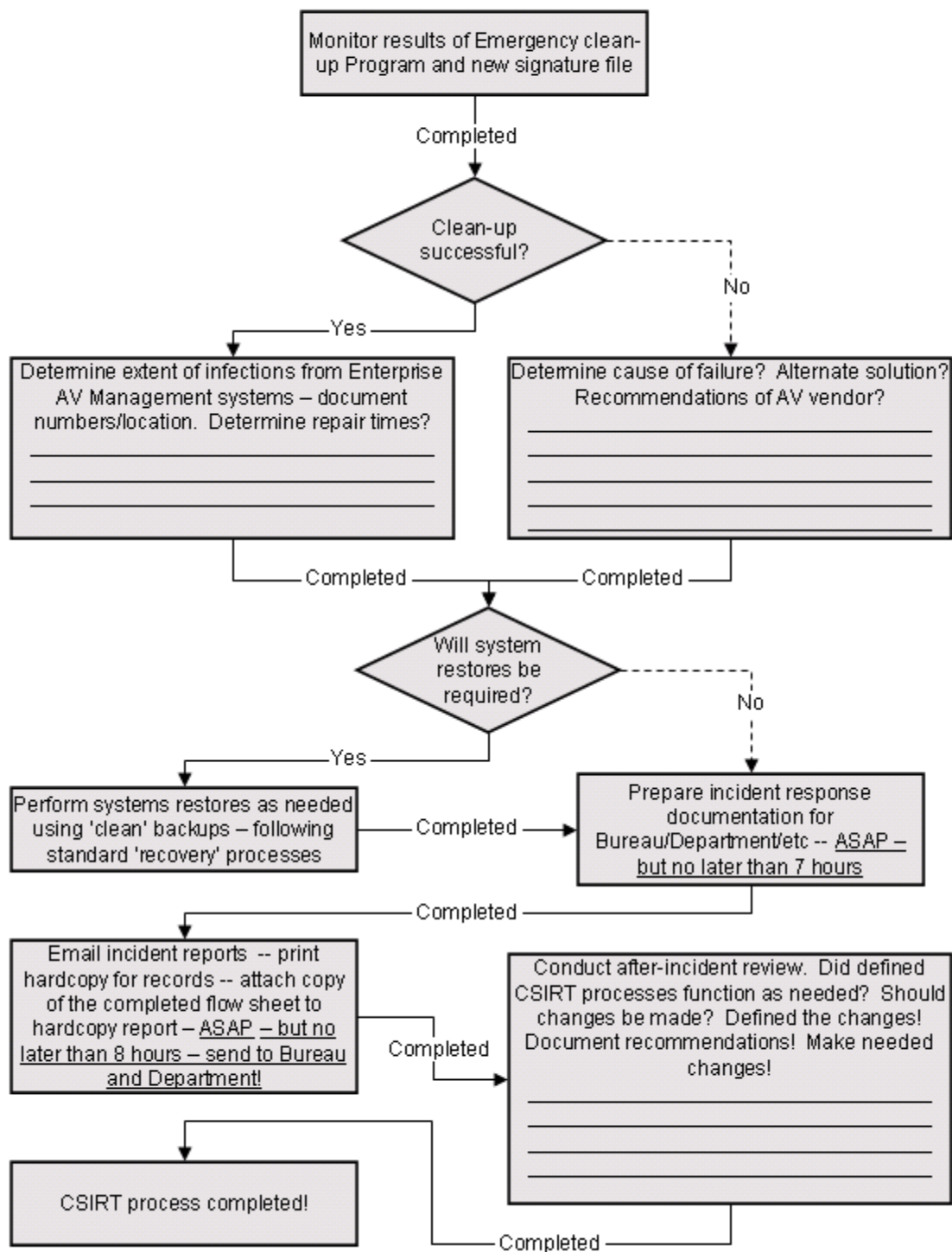


## CSIRT Malware Flowchart

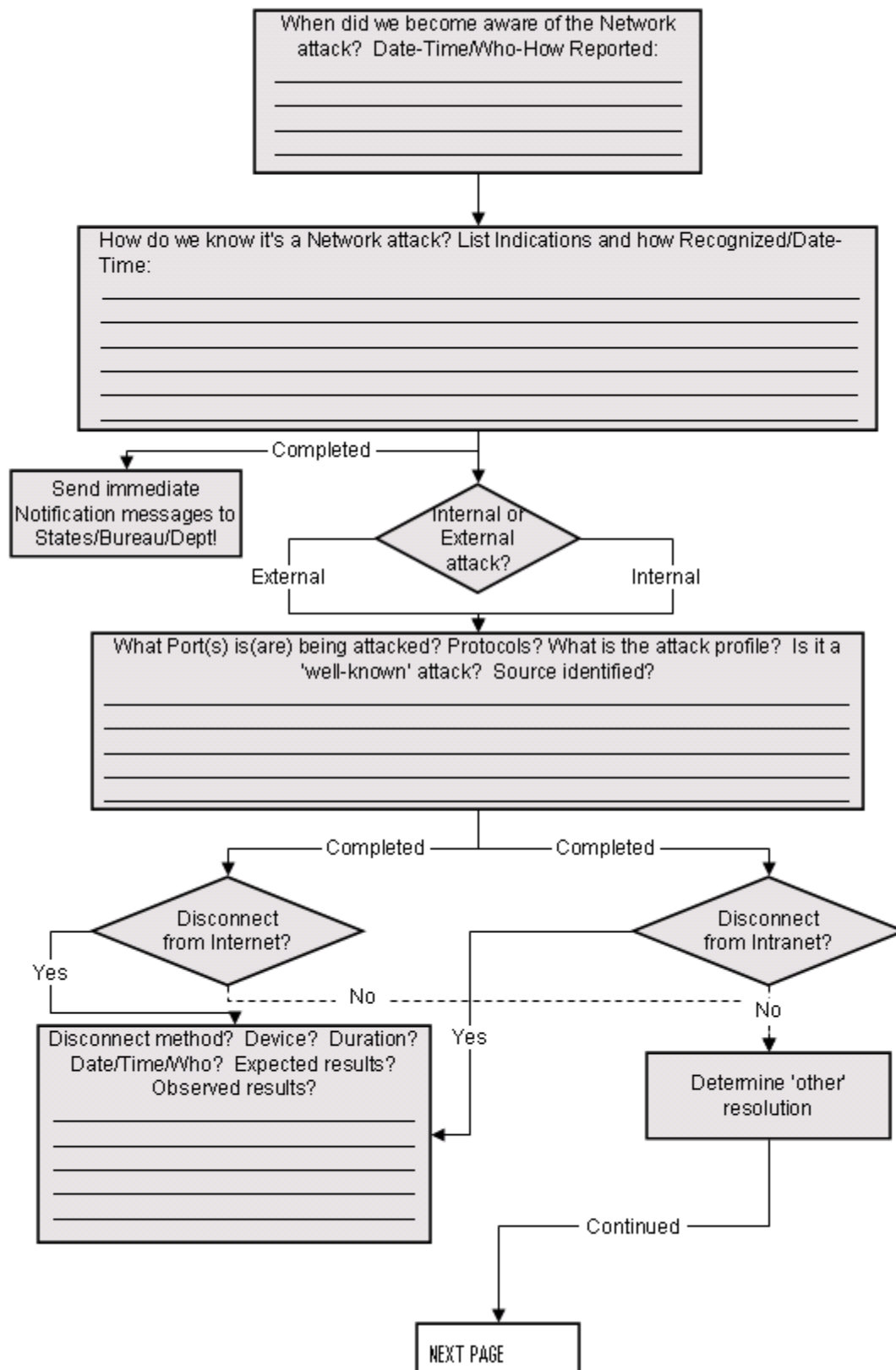




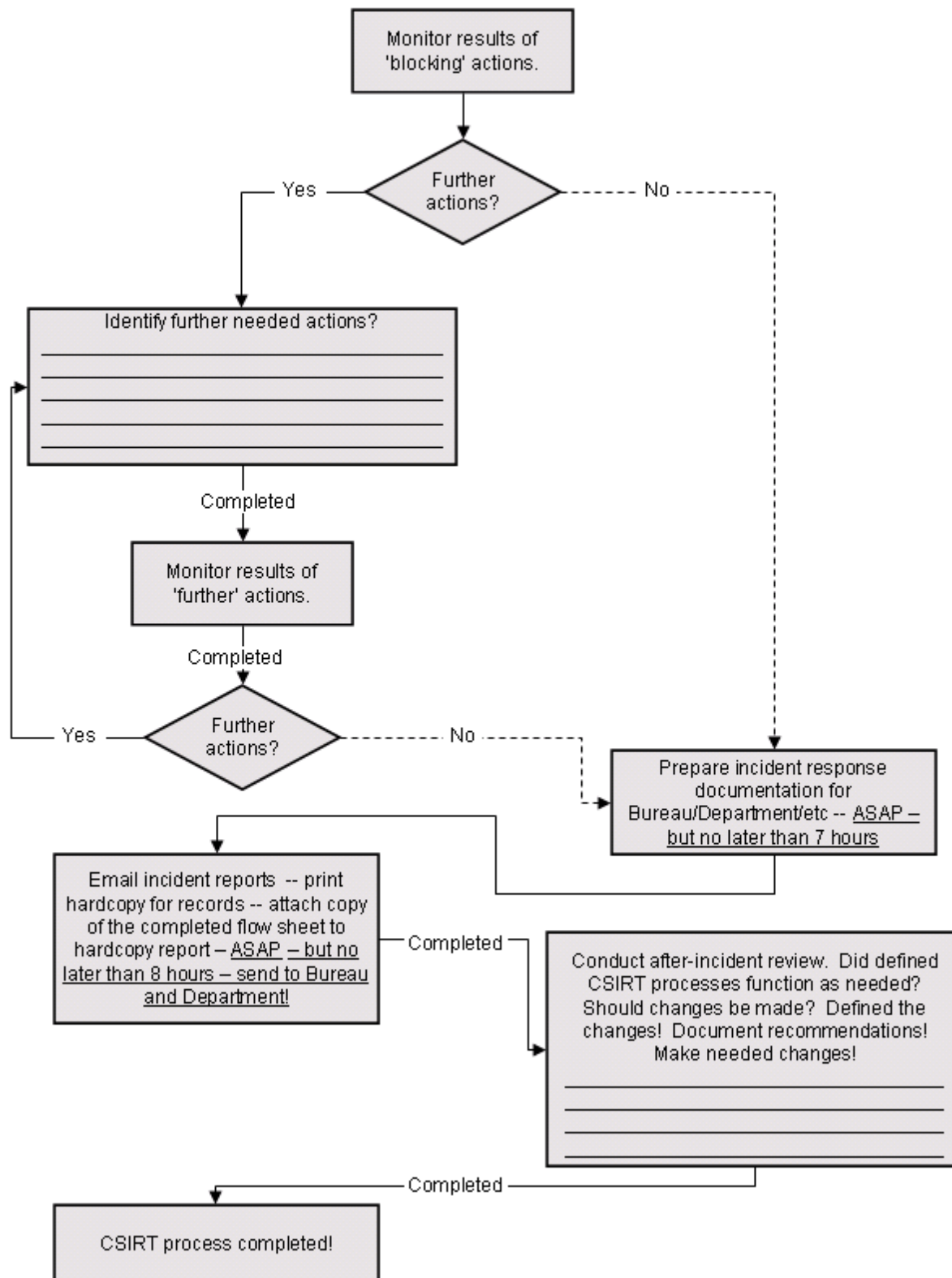
## CSIRT Malware Flowchart



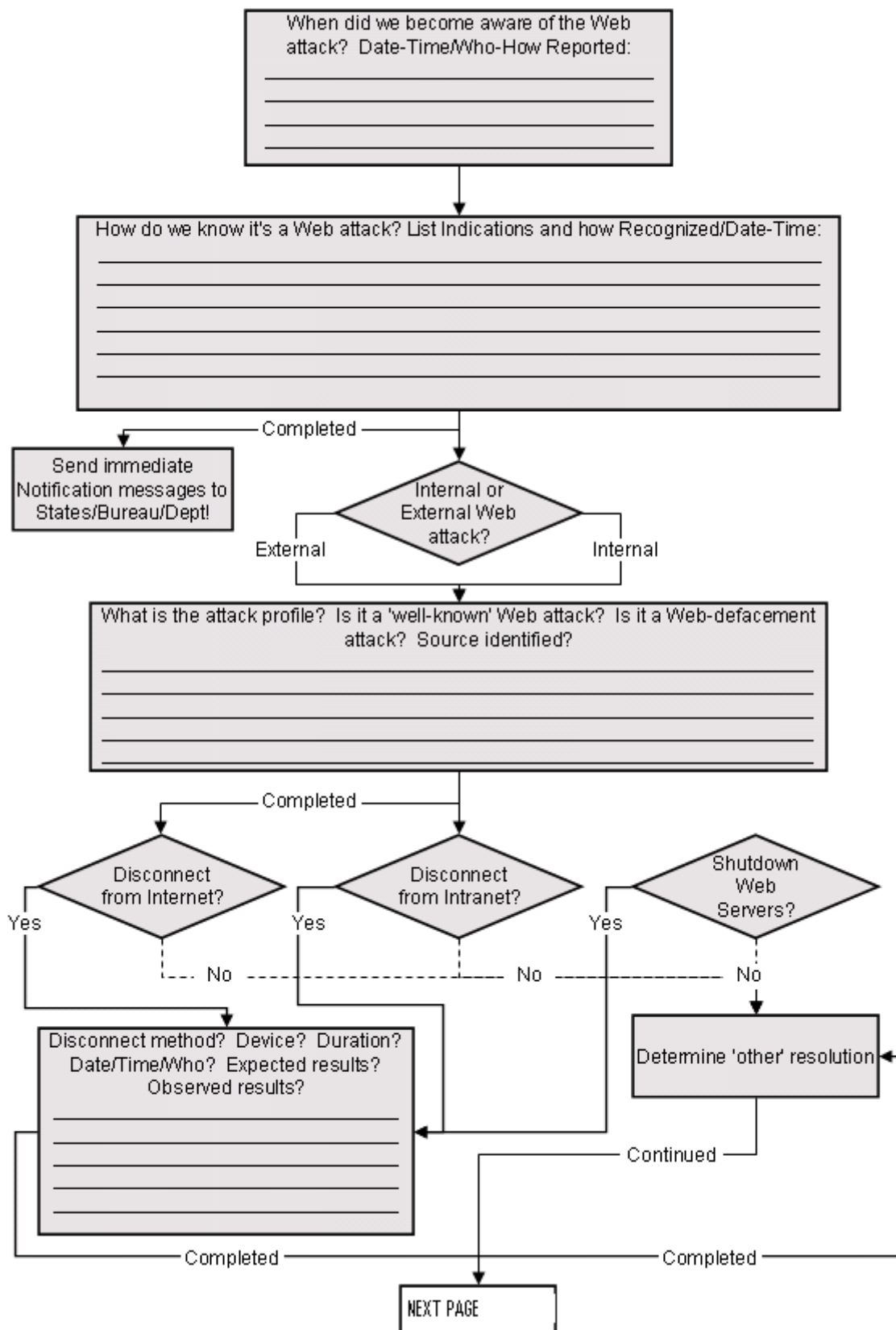
## CSIRT Network Attack Flowchart

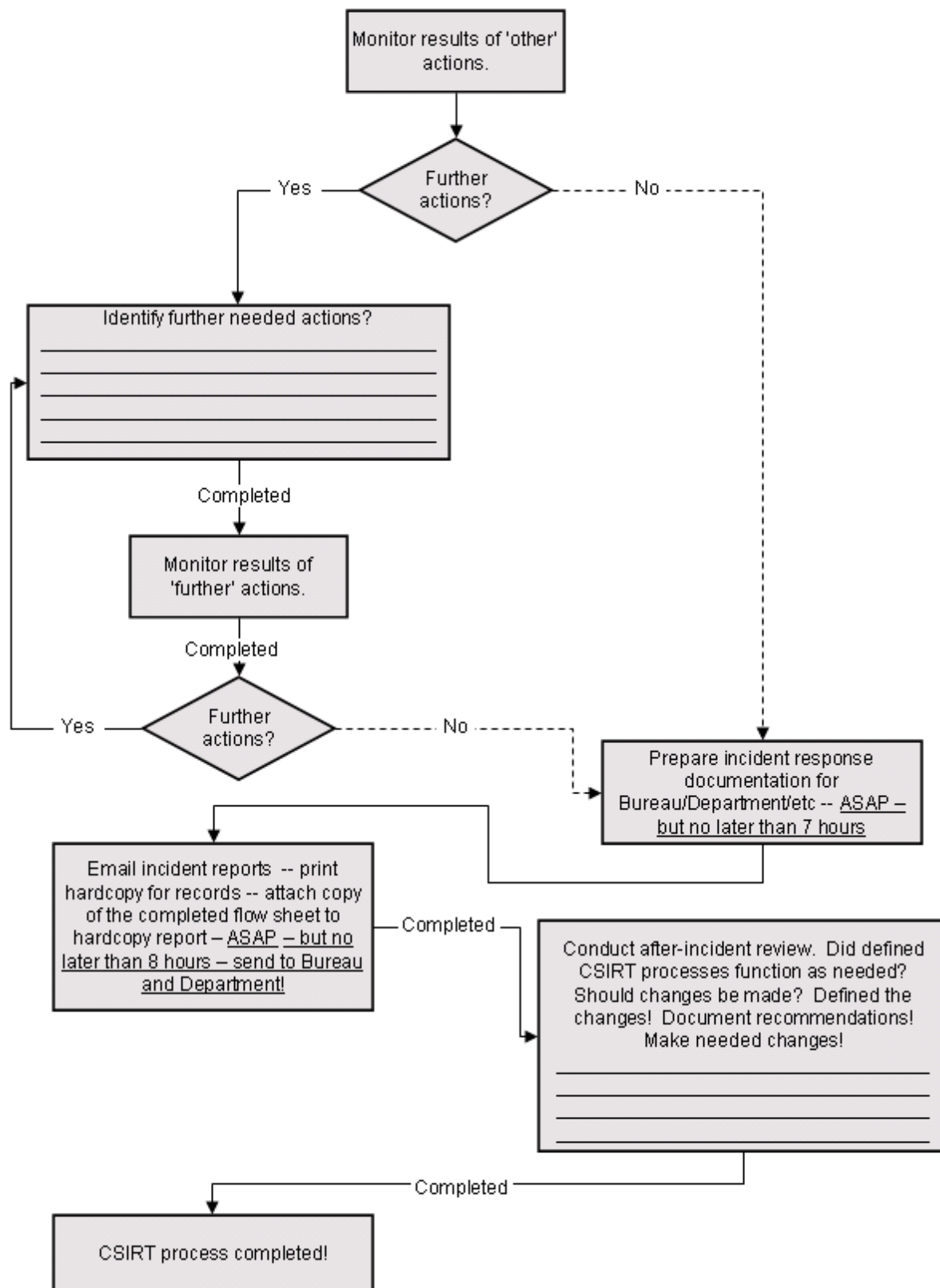


## CSIRT Network Attack Flowchart

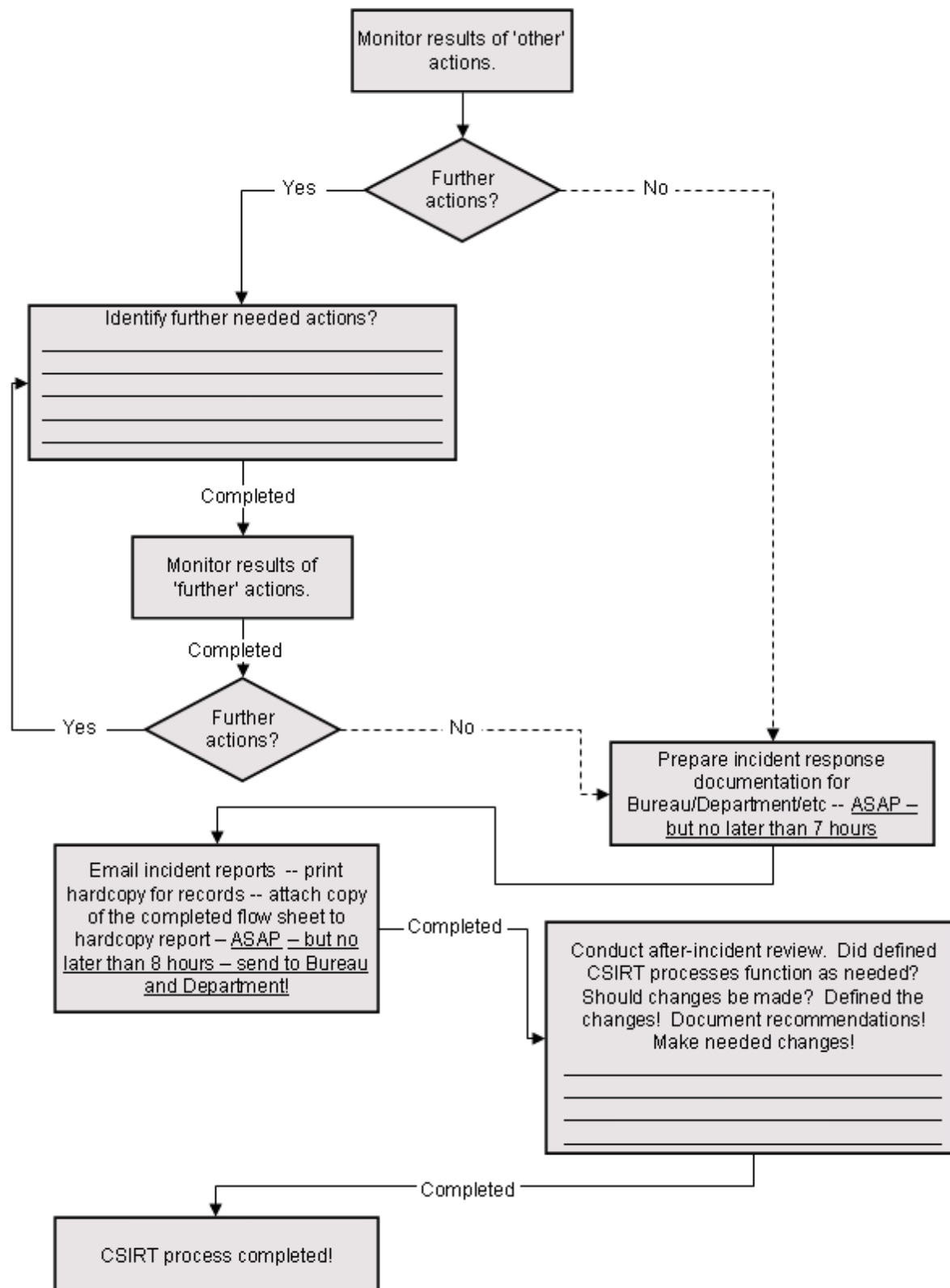


## CSIRT Web Attack Flowchart



**CSIRT Web Attack Flowchart**

## CSIRT Web Attack Flowchart




**APPENDIX C: RISK ASSESSMENT MODEL**

	Factor	Risk Determination	Low Moderate High	Comments: All breaches of PII, whether actual or suspected, require notification to US-CERT through WO-840 staff. Low and Moderate risk/harm determinations and the decision whether notification of individual is made; rest with the Bureau Chief Information Security Officer. All determinations of High risk or harm require notification.
1	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names; those where only one or only a few in the population may have or those who could readily identify an individual, i.e. public figure
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record, and any other information that can be linked or is linkable to an individual
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made
3.	What is the likelihood the information is accessible and usable? What level of protection			

	applied to this information			
	a. Encryption	Low		
	b. Password	Moderate/High		
	c. None	High		
4.	Likelihood the Breach May Lead to Harm	High/Moderate/Low		Determining likelihood depends on the manner of the breach and the types of data involved
5	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been stolen and could possibly be used to commit theft?
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise w/in DOI control	Low/High		No evidence of malicious intent. Evidence or possibility of malicious intent
	(2) Compromise beyond DOI control	High		Possibility that PII could be used with malicious intent or to commit ID theft.



**APPENDIX D: STANDARD BREACH REPORTING TEMPLATE**

		<b>BLM PII Incident Report Template</b>	
<b>Enter Breach Information</b>		<b>Main Point of Contact For More Information:</b>	
Date of Actual Breach (MM/DD/YYYY)	<input type="text"/>	POC First Name	<input type="text"/>
Date of Breach Discovery (MM/DD/YYYY)	<input type="text"/>	POC Last Name	<input type="text"/>
US-Cert Date Reported (MM/DD/YYYY)	<input type="text"/>	POC Title	<input type="text"/>
DOI CIRC Number	<input type="text"/>	POC Duty Email	<input type="text"/>
Incident Involved	<input type="text" value="(click to select)"/>	POC Duty Phone	<input type="text"/>
Incident Category	<input type="text" value="(click to select)"/>	<b>Office Name and Mailing Address</b>	
State Office	<input type="text"/>	Address 1	<input type="text"/>
		Address 2	<input type="text"/>
		City	<input type="text"/>
		State	<input type="text"/>
		Zip	<input type="text"/>
<b>Description of breach</b> (Up to 150 words, bullet format is ok.)			
<input type="text"/>			
<b>Describe actions taken in response to the breach</b> (Up to 150 words, bullet format is ok.)			
<input type="text"/>			
<b>If there were previous reports regarding this incident list the dates and ticket numbers of those reports or enter 'None' in the text box</b>		<b>Internal Breach Tracking Number</b>	
<input type="text"/>		<input type="text"/>	
<b>Was this breach the result of a willful and intentional act?</b>		<input type="radio"/> YES <input type="radio"/> NO	
<b>Number of Individuals Affected:</b>			
# BLM Employees	<input type="text"/>		
# Other Bureau Employees	<input type="text"/>		
# Government Contractors	<input type="text"/>		
# Civilians	<input type="text"/>		
# Other (specify below)	<input type="text"/>		

Number of Individuals from Other DOI Bureaus:	
# DOI Employees	<input type="text"/>
# BIA Employees	<input type="text"/>
# NPS Employees	<input type="text"/>
# FWS Employees	<input type="text"/>
# BOEMRE Employees	<input type="text"/>
# USBR Employees	<input type="text"/>
# USGS Employees	<input type="text"/>
# Other (specify below)	<input type="text"/>

Individuals Notified?	<input type="radio"/> YES <input type="radio"/> NO	If there was no notification explain why
<input type="text"/>		

Notification Date (MM/DD/YYYY)	<input type="text"/>
Credit Monitoring Offered?	<input type="radio"/> YES <input type="radio"/> NO

Type of Personally Identifiable Information involved in the incident:	
Social Security Numbers	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>
Names	<input type="checkbox"/>
Home Addresses	<input type="checkbox"/>
Personal email address	<input type="checkbox"/>
Home Telephone	<input type="checkbox"/>
Protected Health Information (PHI)	<input type="checkbox"/>
Passwords	<input type="checkbox"/>
*Financial Information	<input type="checkbox"/>
Other (specify below)	<input type="text"/>

If Financial Information is selected more specification is needed:	
Personal Credit Card Information	<input type="checkbox"/>
Personal Finance Information	<input type="checkbox"/>
Loan Account Information	<input type="checkbox"/>
**Government Credit Card Information	<input type="checkbox"/>
Government CC issuing bank WAS notified	<input type="checkbox"/>
Government CC issuing bank WAS NOT notified	<input type="checkbox"/>
Other (specify below)	<input type="text"/>

\* if you select Financial Information enter additional details

\*\* if you select Government Credit Card also select if the issuing bank WAS notified or WAS NOT notified.

Select all of the following that apply to the incident	
Paper Records	<input type="checkbox"/>
Record Disposal	<input type="checkbox"/>

If Paper Records or Record Disposal was selected provide more detail	
Paper records faxed or mailed accidentally	<input type="text"/>
Paper records disposed of improperly	<input type="text"/>
Unauthorized disclosure of paper records	<input type="text"/>
Documents posted to internet	<input type="text"/>
Documents posted to intranet	<input type="text"/>

Equipment	<input type="checkbox"/>	If Equipment was selected provide more detail	
Location of equipment	(click to select)		
Equipment owner	(click to select)		
Government equipment DAR encrypted	(click to select)		
Government equipment password or SmartCard protected	(click to select)		
Personal equipment commercially encrypted	(click to select)		
Personal equipment password protected	(click to select)		
Equipment Involved	# of items		
Laptop			
Cell Phone			
PDA			
MP3 player			
Printer/Copier			
Desktop computer			
Flash drive /removeable media			
External hard drive			
Network Intrusion			
Other (specify below)			
Email	<input type="checkbox"/>		
Info Sharing	<input type="checkbox"/>	If Email or Info Sharing was selected provide more detail	
Email was encrypted	<input type="radio"/> YES	<input type="radio"/> NO	
Email was digitally signed	<input type="radio"/> YES	<input type="radio"/> NO	
Email was sent outside the DoJ	<input type="radio"/> YES	<input type="radio"/> NO	
Email recipients non-Federal agency	<input type="radio"/> YES	<input type="radio"/> NO	
Information was:			
posted to the Internet	<input type="radio"/> YES	<input type="radio"/> NO	
posted to an Intranet	<input type="radio"/> YES	<input type="radio"/> NO	
saved on a share drive	<input type="radio"/> YES	<input type="radio"/> NO	
disclosed verbally	<input type="radio"/> YES	<input type="radio"/> NO	
Type of Investigation		Impact Determination is:	
Internal	<input type="checkbox"/>	low	<input type="radio"/>
Local Law Enforcement	<input type="checkbox"/>	medium	<input type="radio"/>
Inspector General	<input type="checkbox"/>	high	<input type="radio"/>
Other (specify below)	<input type="checkbox"/>		
		Is there an associated System of Record?	<input type="radio"/> YES <input type="radio"/> NO
		if the answer is yes, enter the System of Record Number	
Additional Notes (up to 150 words, bullet format is ok)			

Use the **File/Save As** option to choose an .xls or .xlsx format to save the breach report. If you close the template without using the Save As option nothing will be saved.

## APPENDIX E: SAMPLE WRITTEN NOTIFICATION

Dear:

We are writing to you because of a recent security incident at [name of responsible bureau or office]. [Describe what happened in general terms, what kind of Personally Identifiable Information was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on [your credit files (credit card companies, personal banking institutions, etc.)] or [your credit files with the three (3) major credit reporting agencies]. A fraud alert lets creditors know to contact you before opening new accounts. You can contact any one of the three credit reporting agencies at a number or website below to have a fraud alert placed on your account (you may be asked to contact other financial institutions separately). This will allow you to place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each. Alternatively, you can request copies of your credit reports once a year for free online through [www.annualcreditreport.com](http://www.annualcreditreport.com).

Experian

888-397-3742

[www.experian.com](http://www.experian.com)

Equifax

800-525-6285

[www.equifax.com](http://www.equifax.com)

TransUnion

800-680-7289

[www.transunion.com](http://www.transunion.com)

When you receive the credit reports, look them over carefully for accounts you did not open. Also, look for inquiries from creditors that you did not initiate. In addition, look for personally identifiable information, such as home addresses and Social Security numbers that are not accurate.

If you see anything you do not understand, contact the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [Alternatively, if appropriate, give contact number for law enforcement agency investigating the incident for you.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

[Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Contact one of the credit reporting agencies above to order your reports and keep the fraud alert in place.] For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at <http://www.consumer.gov/idtheft>.

If you need further assistance, please contact [name and telephone number of responsible bureau or office] between the hours of \_\_\_\_ and \_\_\_\_ [EST].

[Closing]

## **APPENDIX F: GUIDANCE: ESTABLISH CALL CENTER - PRIVACY ACT BREACH**

In the event of a significant privacy breach of Personally Identifiable Information (PII) the following guidance is provided as the BITTF or Interior ITTF considers whether to establish a call center to handle inquiries related to the incident. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the spillage and possible actions they may want to take to lessen the incident's impact on their personal lives (i.e., identity theft, etc.).

The decision to establish a call center should be based on several considerations:

- If a bureau has a privacy breach that does not extend outside the organization (i.e., those affected by the breach are known and can be contacted), then establishment of a call center would not normally be necessary.
- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.
- Each situation will be unique and the decision to establish a call center must be based on the individual circumstances. The main concern should be the sharing of information with those affected and how they may obtain assistance.
- Once the decision is made to establish a call center there are several follow-up options:
  - Contact the Interior Business Center (IBC) to obtain a toll-free number. This option is most likely the least expensive, since the impacted bureau will be providing its own personnel to staff the call center.
  - Contact the General Services Administration's (GSA) USA Services Group to establish a call center supported and manned by GSA personnel. A statement of work (SOW) will be required and the call center can be up and running usually within 72 hours. SOW requirements can be found at <http://www.gsa.gov/portal/content/103361>. A generic SOW is provided there. A thorough description of the incident and set of frequently asked questions will also be required for GSA personnel to refer to when fielding questions. GSA POCs are: Ms. Barbara Walton at 202-208-0568

Suggested items to consider based on the nature of the breach would include but are not limited to:

- Use of existing bureau personnel to man the call center and the number of individuals required.

- Training of call center operators.
- Pre-staged frequently asked questions (FAQs). Below are questions used during the Veteran's Administrations privacy breach in May 2006. These could be used as a starting point and tailored to meet the requirements of a specific breach.
- Ability to adjust manning in response to call volume.
- Daily hours of operation.
- Cost of service.
- Logging calls.
- Bureau and Department reporting requirements.
- Advertising call center number(s) and making breach information readily available to those affected (i.e., on bureau's and other appropriate websites, mass emailing(s) to those affected, news media, etc.).
- Department periodic check of call center quality of customer service.
- Criteria to disestablish call center.
- Ensure training procedures are in place to prevent additional inadvertent disclosure of PII or sensitive agency information resulting from legitimate or illegitimate deliberate calls attempting to exploit social engineering weaknesses to gain additional unauthorized access to or disclosure of information.

#### Sample Call Center Frequently Asked Questions:

1. *How can I tell if my information was compromised?*

At this point there is no evidence that any missing data has been used illegally. However, the Bureau of \_\_\_\_\_ is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2. *What is the earliest date at which suspicious activity might have occurred due to this data breach?*

The information was stolen from an employee of the Bureau of \_\_\_\_\_ during the month of \_\_\_\_\_, 20XX. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity during the month of \_\_\_\_\_.

3. *I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?*

The Department of \_\_\_\_\_ strongly recommends that individuals closely monitor their financial statements and visit the Department of \_\_\_\_\_ special website at [www.\\_\\_\\_\\_\\_.gov](http://www._____.gov).

4. *Should I reach out to my financial institutions or will the Department of \_\_\_\_\_ do this for me?*

The Department of \_\_\_\_\_ does not believe that it is necessary to cancel credit cards and bank accounts, unless you detect suspicious activity. However, you should contact your financial institutions (e.g., bank or financial lenders, credit card companies, the Social Security Administration, etc.) to notify them that your PII may have been lost, stolen or obtained by an unauthorized third-party and have a "fraud alert" placed on your accounts/files.

5. *Where should I report suspicious or unusual activity?*

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

- Contact the fraud department of one of the three major credit bureaus:

Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241.

Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, Texas 75013.

TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Close any accounts that have been tampered with or opened fraudulently.
- File a police report with your local police or the police in the community where the identity theft took place.
- File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by telephone: 1-877-438-4338, online at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

6. *I know the Department of \_\_\_\_\_ maintains my health records electronically. Was this information also compromised?*

No electronic medical records were compromised. The data lost is primarily limited to an individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of potential use to identity thieves and we recommend that all individuals be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7. *What is the Department of \_\_\_\_\_ doing to ensure that this does not happen again?*

The Department of \_\_\_\_\_ is working with the President's Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate this data breach and to develop safeguards against similar incidents. The Department of \_\_\_\_\_ has directed all employees to complete the "DOI Cyber Security Awareness Training Course" and complete the separate "DOI Employee Privacy Awareness Course" by \_\_\_\_\_, 20XX. In addition, the Department of \_\_\_\_\_ will immediately be conducting an inventory and review of all current positions requiring access to sensitive data and require all employees requiring access to sensitive data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the Inspector General of the Department of \_\_\_\_\_, have launched full-scale investigations into this matter.

8. *Where can I get further, up-to-date information?*

The Department of \_\_\_\_\_ has set up a special website and a toll-free telephone number for employees that feature up-to-date news and information. Please visit [www.\\_\\_\\_\\_\\_.gov](http://www._____.gov) or call 1-800-XXX-XXXX.

9. *Does the electronic data theft affect only \_\_\_\_\_?*

It potentially affects all employees hired since \_\_\_\_\_, which is when automated records management began and regular input of information commenced.

We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.



**APPENDIX G: SAMPLE AFTER ACTION REPORT*****AFTER ACTION REPORT*****DOI CIRC Incident #1111, (Incident Location or System)****FACTS:**

*(In this section the basic facts of the incident should be detailed to include causes, issues, actions taken, etc. should be detailed. All details that could assist in preventing other incidents or that underscore why a particular action was needed or taken should be included. See paragraph 3.7, Phase 7: Learn from the Incident)*

**LESSONS LEARNED:** *(In this section the basic issues or problems that caused the incident or arose from the incident should be detailed. The format below is a suggestion. The lessons should be organized in the manner most efficient for imparting the information).*

**A. Lesson 1:**

1. Sub-Lesson
2. Sub-Lesson
3. Sub-Lesson

**B. Lesson 2:**

1. Sub-Lesson
2. Sub-Lesson
3. Sub-Lesson

**RECOMMENDATIONS**

Prepared by:  
*(name)(title)(contact information)*

**ATTACHMENTS:**

## **APPENDIX H: PII INCIDENT RESPONSE QUICK REFERENCE**

This quick reference guide provides information regarding how to process incidents involving personally identifiable information (PII) and what actions should be taken in response to the various categories of incidents. This guide is intended as a reference only and does not supersede any written Bureau of Land Management or Department of Interior guidance. Unless otherwise indicated these actions should be taken by the State Privacy Act Officer and/or NOC DIRM Ops Security who has responsibility for the server used to send the PII. If it is suspected that the information was compromised with the intent to commit a crime or in furtherance of criminal activity, contact law enforcement immediately. (NOTE: Contact Law Enforcement does not negate or satisfy the requirement to notify US-CERT within one hour of discovering an incident.) If an incident arises involving the compromise of PII from a source other than receiving a DOI CIRC ticket, both Bureau Privacy Act officer Suzanne Wachter (swachter@blm.gov) and the WO-840 team (BLM\_Incidents\_IT\_Security@blm.gov) should be immediately informed.

### **A. Attempts to send PII**

1. Email is stopped by Symantec Messaging Gateway
2. Incident will be entered into Remedy by WO-840 personnel
3. Remind the individual of the prohibition against sending PII via email unencrypted and provide them a copy of IM 20120504
4. Require them to re-take FISSA+ training and to delete the email off the system
  - a. If training is not accomplished within 3 days restrict the individual's computer access
5. Enter that the user has been counseled and that FISSA+ retraining has been accomplished in the resolution tab of Remedy
6. Once the above steps are complete, notify WO-840 team

### **B. Incidents involving Government Charge Card**

1. Incident entered into DOI CIRC by the WO-840 team
2. State Privacy Officer for the State where the attempt was made has primary responsibility but they should work closely with individual responsible for the government charge card program for their state
3. Notify the individuals whose charge card number have been potentially compromised
4. Ensure all copies of the email and the information has been deleted (from the inbox and deleted email folders)
5. Notify the BLM employee(s) who run the government charge card program for the location where the incident occurred
6. Notify credit card company of the potential breach
7. Determine if the card(s) should be cancelled
8. Remind the individual of the prohibition against sending PII via email unencrypted
9. Require them to retake the FISSA+ training

- a. If training is not accomplished within 3 days restrict the individual's computer access
- 10. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate
- 11. Once all necessary action has been completed, inform WO-840 staff to close incident

### **C. Incidents involving PII**

- 1. Incident entered into DOI CIRC by WO-840 team
- 2. Ensure all copies of the email and the information have been deleted (as appropriate, from the inbox, deleted email folders, computer, servers, etc.)
- 3. Remind the individual of the prohibition against sending PII via email unencrypted
- 4. At a minimum, require the individual to retake the FISSA+ training
  - a. If training is not accomplished within 3 days restrict the individual's computer access
- 5. Convene a Bureau Identity Theft Task Force (BITTF) (see E)
- 6. After a determination had been made by the BITTF that notification is warranted, notify the individual(s) whose PII has been compromised
- 7. The types of notification are discussed below:
  - a. Telephonic notification – small number and the situation dictates urgency
  - b. First-Class Mail notification - most widely accepted, should be mailed separately from other information and marked “Important Notification”
  - c. Email notification – may be used if individuals have consented to the use of email as a primary means of communication with agency and no mailing address is known
  - d. If unique circumstances exist requiring exceptions be made to the above directions or alternative methods of notification need to be used, contact Suzanne Wachter at swachter@blm.gov or 202-912-7627
- 8. Depending on the severity and intent of the incident, disciplinary action against the individual may be appropriate
- 9. Once all necessary action has been completed, inform the WO-840 team to close incident

### **D. Incidents involving Usernames/Passwords**

- 1. Incident entered into DOI CIRC by the WO-840 team
- 2. Remind the individual of the prohibition against sending PII via email unencrypted
- 3. The user will need to change the government usernames and passwords if compromised
- 4. If any administrator usernames/passwords were compromised, the system administrator should be notified
- 5. Require them to retake the FISSA+ training

- a. If training is not accomplished within 3 days restrict the individual's computer access
6. Depending on the severity of the incident, the individual may need to be reprimanded or suspended
7. Once all necessary action has been completed, inform the WO-840 team to close incident

**E. Incidents involving Sensitive BLM Data (financial data, IP addresses, system information, etc.)**

1. Incident entered into DOI CIRC by the WO-840 team
2. Remind the individual of the prohibition against sending sensitive BLM data via email unencrypted
3. Require them to retake the FISSA+ training
  - a. If training is not accomplished within 3 days restrict the individual's computer access
4. Depending on the severity of the incident, the individual may need to be reprimanded or suspended
5. Once all necessary action has been completed, inform the WO-840 team to close incident

**F. BITTF Requirements**

1. Forward information on the incident to the Bureau Privacy Act Officer (Suzanne Wachter, swachter@blm.gov, 202-912-7627)
2. The State Privacy Officer where the incident occurs must schedule a BITTF within 3 business days of the incident
3. The BITTF should include at a minimum:
  - a. Bureau Privacy Act Officer, Suzanne Wachter,
  - b. Bureau Chief Information Security Officer (BCISO)
  - c. Branch Chief, WO-840
  - d. A representative from the Solicitor's Office
  - e. NOC DIRM Ops Security
  - f. A management representative for the division where the breach occurred
4. The following should be invited to the BITTF based on the circumstance of the BITTF
  - a. Human Resources representative
  - b. Public Affairs representative
  - c. Government Charge Card manager
  - d. Law Enforcement
  - e. Internal Affairs/Inspector General
  - f. Supervisor of the individual suspected of committing the breach

5. The Bureau Privacy Act Officer will invite the following people as required, the Deputy Assistant Director, Information Resources Management, DOI Privacy Act Office, and other WO program managers as needed
6. The BITTF should include a conference call option to accommodate geographically separate individuals
7. The BITTF agenda will include the following:
  - a. Perform Initial Assessment of the Incident
  - b. Confirm completion of Appropriate Internal Notifications
  - c. Confirm Involvement of Appropriate Personnel
  - d. Determine Exact Nature of Information Loss
  - e. Analyze Information Loss to Determine Potential Impacts
  - f. Determine Mitigation Plan of Action
  - g. Determine External Notification Plan of Action
  - h. Complete Mitigation and External Notification Activities
  - i. Review Lessons Learned
8. The State Privacy Officer will be responsible for ensuring meeting minutes are taken and WO-840 personnel are kept informed of any updates that should be included in the US-CERT notification
9. BITTFs will be held on a weekly basis until the incident is closed or the BITTF members agree that weekly meetings are no longer necessary

#### **G. Miscellaneous**

1. Notification letters should not be sent when there is a low potential that the individuals whose information was compromise will actually suffer any harm. The potential for harm is determined by considering:
  - a. Nature of the data elements breached (i.e. social security numbers vs home address only)
  - b. Number of individuals affected (mainly considered in type of notification to use)
  - c. Likelihood the information is accessible and useable
  - d. Likelihood the breach may lead to harm
  - e. Ability of the Agency to mitigate the risk or harm
2. Credit Monitoring should also only be offered in cases where there is a high potential for harm to the affected individuals
3. Public affairs should be informed of major incidents so that they can determine whether a press release is needed